

国際調査報告

(法 8 条、法施行規則第40、41条)
〔PCT 18条、PCT規則43、44〕

出願人又は代理人 の書類記号 522214WO01	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。		
国際出願番号 PCT/JPO0/09128	国際出願日 (日.月.年) 22.12.00	優先日 (日.月.年) 27.12.99	
出願人 (氏名又は名称) 三菱電機株式会社			

国際調査機関が作成したこの国際調査報告を法施行規則第41条 (PCT 18条) の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない (第 I 欄参照)。

3. ☐ 発明の単一性が欠如している (第 II 欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第 III 欄に示されているように、法施行規則第47条 (PCT 規則38.2(b)) の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から 1 カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 9 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int. Cl. ⁷ H04Q 7/38 H04L 9/16		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int. Cl. ⁷ H04B 7/24-7/26 H04Q 7/00 G09C 1/00-5/00 H04K 1/00-3/00 H04L 9/00		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 10-22996, A (三菱電機株式会社) 23. 1月. 1998 (23. 01. 98) & GB, 2314741, A & CA, 2205637, A & DE, 19721949, A1 & US, 6016350, A	1-38
Y	JP, 7-245606, A (日本電気株式会社) 19. 9月. 1995 (19. 09. 95), (ファミリーなし)	1-38
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 12. 03. 01	国際調査報告の発送日 21.03.01	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 丸山 高政 電話番号 03-3581-1101 内線 3574	

THIS PAGE BLANK (USPTO,

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 7-327257, A (株式会社日立製作所) 12. 12月. 1995 (12. 12. 95), (ファミリーなし)	1-38
Y	J P, 10-66157, A (ノキア モービル フォーンズ リミティド) 6. 3月. 1998 (06. 03. 98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111, A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	J P, 5-22284, A (国際電気株式会社) 29. 1月. 1993 (29. 01. 93), (ファミリーなし)	1-38
Y	D. W. Davies and W. L. Price著, 上園忠弘監訳 「ネットワーク・セキュリティ」日経マグロウヒル, (昭和60年), pp. 77-78及び121-123	9, 18, 24-26

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09128

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04Q 7/38, H04L 9/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04B 7/24-7/26, H04Q 7/00, G09C 1/00-5/00,
H04K 1/00-3/00, H04L 9/00Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-22996, A (Mitsubishi Electric Corporation), 23 January, 1998 (23.01.98) & GB, 2314741, A & CA, 2205637, A & DE, 19721949, A1 & US, 6016350, A	1-38
Y	JP, 7-245606, A (NEC Corporation), 19 September, 1995 (19.09.95) (Family: none)	1-38
Y	JP, 7-327257, A (Hitachi, Ltd.), 12 December, 1995 (12.12.95) (Family: none)	1-38
Y	JP, 10-66157, A (Nokia Mobile Phones Ltd.), 06 March, 1998 (06.03.98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111, A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	JP, 5-22284, A (Kokusai Electric Co., Ltd.), 29 January, 1993 (29.01.93) (Family: none)	1-38

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to
"A" document defining the general state of the art which is not considered to be of particular relevance	understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
12 March, 2001 (12.03.01)Date of mailing of the international search report
21 March, 2001 (21.03.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	D. W. Davies and W. L. Price; Translation supervised by Tadahiro Uezono "Network Security", Nikkei McGraw Hill (1985), pp. 77-78, pp.121-123	9, 18, 24-26

THIS PAGE BLANK (USPTO)

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年7月5日 (05.07.2001)

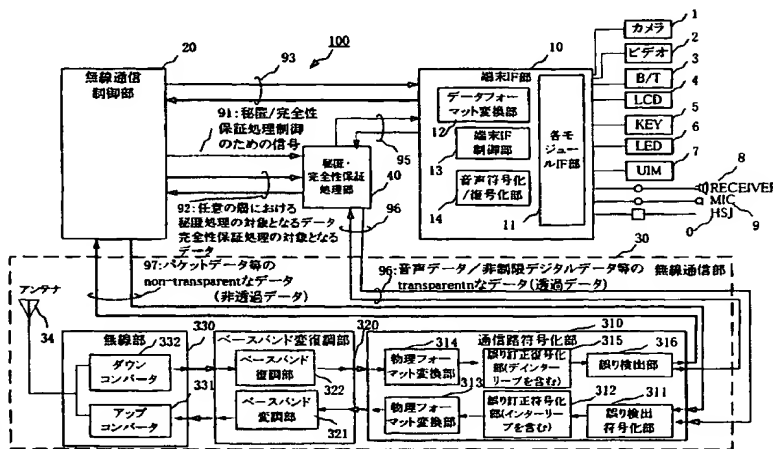
PCT

(10) 国際公開番号
WO 01/49058 A1

- (51) 国際特許分類: H04Q 7/38, H04L 9/16 (30) 優先権データ:
特願平 11/370657
- (21) 国際出願番号: PCT/JP00/09128 1999年12月27日 (27.12.1999) JP
- (22) 国際出願日: 2000年12月22日 (22.12.2000) (71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (72) 発明者; および (75) 発明者/出願人 (米国についてのみ): 宇賀晋介 (UGA, [続葉有])

(54) Title: RADIO COMMUNICATION DEVICE AND RADIO COMMUNICATION METHOD

(54) 発明の名称: 無線通信装置及び無線通信方法



- 20...RADIO COMMUNICATION CONTROL UNIT
91...SIGNAL FOR CONTROL OF SECRETING/COMPLETENESS-SECURING
40...SECRETING/COMPLETENESS-SECURING UNIT
92...DATA TO BE SECRETED IN ANY LAYER AND DATA THE COMPLETENESS OF WHICH IS TO BE SECURED
10...TERMINAL IF UNIT
12...DATA FORMAT CONVERTING SECTION
13...TERMINAL IF CONTROL SECTION
14...AUDIO ENCODING/DECODING SECTION
11...MODULE IF SECTIONS
1...CAMERA
2...VIDEO
97...NON-TRANSPARENT DATA SUCH AS PACKET DATA
96...TRANSPARENT DATA SUCH AS AUDIO DATA/NON-LIMITED DATA
30...RADIO COMMUNICATION UNIT
34...ANTENNA
330...RADIO SECTION
332...DOWN CONVERTER
331...UP CONVERTER
320...BASEBAND MODULATING/DEMULATING SECTION
322...BASEBAND DEMODULATING PART
321...BASEBAND MODULATING PART
310...COMMUNICATION LINE ENCODING SECTION
314...PHYSICAL FORMAT CONVERTING PART
313...PHYSICAL FORMAT CONVERTING PART
315...ERROR CORRECTION DECODING PART (INCLUDING DEINTERLEAVING)
312...ERROR CORRECTION ENCODING PART (INCLUDING INTERLEAVING)
316...ERROR DETECTING SECTION
311...ERROR DETECTING/CORRECTING PART

(57) Abstract: A radio terminal (MS) (100) capable of secreting and securing completeness in layer 2 or higher-order layers and comprising a terminal IF unit (10), a radio communication control unit (20), a radio communication unit (30), and a secreting/completeness-securing unit (40) connected to the terminal IF unit (10), the terminal IF unit (20), and the radio communication unit (30). The secreting/completeness-securing unit (40) only secrets transparent data such as audio data with respect to the terminal IF unit (10) and the radio communication unit (30), secrets non-transparent data and/or secures the completeness of the nontransparent data with respect to the radio communication control unit (20), and selectively secrets data on layer 2 and the higher-order layers outputted from the radio communication unit (30) or secures the completeness of the data according to the type of data.

[続葉有]



Shinsuke) [JP/JP]. 松山浩司 (MATSUYAMA, Hiroshi) [JP/JP]. 近澤 武 (CHIKAZAWA, Takeshi) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井章司, 外(MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).

(81) 指定国 (国内): AU, CA, CN, JP, KR, MX, NO, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

レイヤ2以上の上位レイヤにおいて秘匿処理及び完全性保証処理が行える無線端末(MS)100を提供したい。端末IF部10と無線通信制御部20と無線通信部30との間に秘匿・完全性保証処理部40を設ける。秘匿・完全性保証処理部40は、端末IF部10と無線通信部30との間で音声データ等の透過データに対して秘匿処理のみを行う。秘匿・完全性保証処理部40は、無線通信制御部20との間で非透過データに対して秘匿処理又は/及び完全性保証処理を行う。秘匿・完全性保証処理部40は、無線通信部30から出力されたレイヤ2以上の上位階層のデータに対してデータの種別に応じて選択的に秘匿処理、完全性保証処理を行う。

明 細 書

無線通信装置及び無線通信方法

5 技術分野

この発明は、携帯電話機等の無線通信装置及び無線通信方法に関するものである。特に、データの秘匿処理と完全性保証処理を行う携帯電話機に関するものである。

10 背景技術

図24は、従来の携帯電話機500を示す図である。

従来の携帯電話機500には、端末IF（インタフェース）部510と無線通信制御部520と無線通信部530が備えられている。端末IF部510は、携帯電話機500のユーザとのインタフェースを行う部分である。無線通信制御部520は、携帯電話機500全体の通信制御とプロトコルに基づくデータの変換とデータ処理とを行う部分である。無線通信部530は、データを変調復調し、無線通信可能とする部分である。無線通信部530は、OSI（Open Systems Interconnection）で定義されている7階層のレイヤの内、
15 最下層である物理レイヤ（レイヤ1）をサポートしている部分である。無線通信部530には、秘匿処理部540が設けられている。秘匿処理部540は、無線通信部530で取り扱われる物理レイヤのデータに対して暗号化処理、或いは、復号化処理を行う部分である。秘匿処理部540を設けることによりアンテナ541で送受信されるデータを盗聴し
20 ても暗号化されているので、解読されない限りにおいて盗聴者が有意な情報を得ることはできないこととなる。

従来の携帯電話機 500 は、秘匿処理部 540 を無線通信部 530 の内部に有している。このため、秘匿処理部 540 が秘匿対象とするデータは、物理レイヤ（レイヤ 1）のデータである。物理レイヤでは、そのデータがユーザデータであるか制御データであるかは特定できない。携帯電話機により送受信されるデータの中には、各種ユーザデータ及びシグナリングデータなどいろいろな種類があり、そのデータの種類に応じて秘匿処理を行ったり、或いは、そのデータの重要性に応じてデータの完全性を保証したりする必要がある。従来の構成のように、秘匿処理部 540 がレイヤ 1 に設けられていたのでは、レイヤ 1 においてはデータの種別が区別できないため、データの種別に応じて秘匿処理や完全性の保証をするということができなかった。

この発明の好適な実施の形態では、データの種類に応じて秘匿処理や完全性保証処理が選択的に行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、OSI の 7 つの階層の内、レイヤ 2（データリンク層）以上の上位レイヤにおいて秘匿処理と完全性保証処理が行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、秘匿処理と完全性保証処理との両方又は一方をデータの種類に応じて選択的に行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、無線通信装置が複数のチャネルを有している場合においてもチャネル毎に秘匿処理と完全性保証処理とが行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、あるレイヤ、或いは、サブレイヤを透過する透過データと、そのレイヤ、或いは、サブレイヤを透

過しない非透過データとを区別して、秘匿処理と完全性保証処理とを選択的に行う無線通信装置及び無線通信方法を得ることを目的とする。

発明の開示

5 この発明に係る無線通信装置は、データを入力する端末インタフェース部と、

 端末インタフェース部が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

 無線通信制御部から制御信号とデータとを入力し、入力した制御信号
10 に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

 無線通信制御部から出力されたデータを入力して変調し送信する無線
15 通信部と
 を備えたことを特徴とする。

 上記秘匿・完全性保証処理部は、

 無線通信制御部から制御信号を入力し、入力した制御信号に基づいて
20 端末インタフェース部からデータを選択的に入力するとともに、
 入力したデータに対して秘匿処理を行い、
 秘匿処理したデータを無線通信部に出力することを特徴とする。

 上記端末インタフェース部は、透過データと非透過データとを出力し
25 、

 上記無線通信制御部は、非透過データを端末インタフェース部から入

力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを端末インタフェース部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする。

- 5 上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする。

- 10 上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする。

- 15 上記秘匿・完全性保証処理部は、
入力したデータを暗号化する暗号化部を有する秘匿処理部と、
入力したデータに対して完全性認証子を付加する完全性認証子付加部
を有する完全性保証処理部と
を備えたことを特徴とする。

上記秘匿処理部は、複数の暗号化部を有することを特徴とする。

- 20 上記完全性保証処理部は、複数の完全性認証子付加部を有することを特徴とする。

- 25 上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する1つのモジュールであり、その1つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部のいずれかの処理を実行するこ

とを特徴とする。

この発明に係る無線通信装置は、データを受信して復調する無線通信部と、

- 5 無線通信部により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行
10 い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

無線通信制御部により処理されたデータを入力して出力する端末インタフェース部と
を備えたことを特徴とする。

15

上記秘匿・完全性保証処理部は、

無線通信制御部から制御信号を入力し、入力した制御信号に基づいて無線通信部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

- 20 秘匿処理したデータを端末インタフェース部に出力することを特徴とする。

上記無線通信部は、透過データと非透過データとを出力し、

- 25 上記無線通信制御部は、非透過データを無線通信部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを無線通信部から秘匿・完全性保証処理部に入力させて秘匿処理

させることを特徴とする。

上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする。

5

上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする。

10

上記秘匿・完全性保証処理部は、
入力したデータを復号化する復号化部を有する秘匿処理部と、
入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部を有する完全性保証処理部と
を備えたことを特徴とする。

15

上記秘匿処理部は、複数の復号化部を有することを特徴とする。

上記完全性保証処理部は、複数の完全性確認部を有することを特徴とする。

20

上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する1つのモジュールであり、その1つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行すること

25

とを特徴とする。

この発明に係る無線通信装置は、データを無線通信する無線通信装置において、

データを入出力する端末インタフェース部と、

プロトコルに基づいてデータの処理をする無線通信制御部と、

5 データを無線通信する無線通信部と、

端末インタフェース部と無線通信制御部と無線通信部との三者間に設けられ、無線通信制御部との間でデータに対して少なくともデータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース部から無線通信部へのデータ
10 データを暗号化するとともに無線通信部から端末インタフェース部へのデータを復号する秘匿・完全性保証処理部とを備えたことを特徴とする。

上記秘匿・完全性保証処理部は、

15 入力したデータに対して秘匿処理を行う秘匿処理部と、

入力したデータに対して完全性保証処理を行う完全性保証処理部とを個別に備えたことを特徴とする。

上記秘匿処理部は、

20 端末インタフェース部から無線通信部へのデータを暗号化する暗号化部と、

無線通信部から端末インタフェース部へのデータを復号化する復号化部とを個別に有することを特徴とする。

25 上記完全性保証処理部は、

入力したデータに対して完全性保証処理を行う完全性認証子を付加す

る完全性認証子付加部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部と
を個別に有することを特徴とする。

5

上記通信装置は、携帯型移動電話機であることを特徴とする。

上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする。

10

上記無線通信装置は、携帯電話機であることを特徴とする。

上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする。

15

上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする。

20

この発明に係る無線通信方法は、データを入力する端末インタフェース工程と、

端末インタフェース工程が入力したデータを入力し、データを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

25

無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全

性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

無線通信制御工程から出力されたデータを入力して変調し送信する無線通信工程と

5 を備えたことを特徴とする。

この発明に係る無線通信方法は、データを受信して復調する無線通信工程と、

無線通信工程により復調されたデータを入力して、プロトコルに基づ
10 いてデータを処理して出力する無線通信制御工程と、

無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保
15 証処理工程と、

無線通信制御工程により処理されたデータを入力して出力する端末インタフェース工程と
を備えたことを特徴とする。

20 この発明に係る無線通信方法は、データを無線通信する無線通信方法において、

データを入出力する端末インタフェース工程と、

プロトコルに基づいてデータの処理をする無線通信制御工程と、

データを無線通信する無線通信工程と、

25 端末インタフェース工程と無線通信制御工程と無線通信工程との三者間に設けられ、無線通信制御工程との間でデータに対して少なくともデ

ータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース工程から無線通信工程へのデータを暗号化するとともに無線通信工程から端末インタフェース工程へのデータを復号する秘匿・完全性保証処理工程と

5 を備えたことを特徴とする。

図面の簡単な説明

図 1 は、移動体通信システムの構成図。

図 2 は、無線制御局（RNC）120の構成図。

10 図 3 は、実施の形態 1 の無線端末（MS）100の構成図。

図 4 は、実施の形態 1 の秘匿・完全性保証処理部 40の構成図。

図 5 は、実施の形態 1 の秘匿・完全性保証処理部 40の構成図。

図 6 は、実施の形態 1 の秘匿・完全性保証処理部 40の構成図。

図 7 は、実施の形態 1 の秘匿・完全性保証処理部 40の構成図。

15 図 8 は、実施の形態 1 の秘匿・完全性保証処理部 40の構成図。

図 9 は、実施の形態 2 の無線端末（MS）100の構成図。

図 10 は、実施の形態 2 の秘匿・完全性保証処理部 40の構成図。

図 11 は、実施の形態 2 の秘匿・完全性保証処理部 40の構成図。

図 12 は、暗号化方式及び復号化方式の一例を示す図。

20 図 13 は、実施の形態 2 の秘匿・完全性保証処理部 40の構成図。

図 14 は、ARIB STD-T63 33.102, 3G Security; Security Architecture, Section 6.3. に示された図。

25 図 15 は、ARIB STD-T63 33.102, 3G Security; Security Architecture, Figure 16b. に示された図。

図16は、ARIB STD-T63 33.102, 3G Security; Security Architecture, Figure 16. に示された図。

図17は、暗号化／復号化部421の中で用いられる暗号化モジュール51（又は復号化モジュール71）の構成図。

図18は、秘匿・完全性保証処理部40の実装形式を示す図。

図19は、秘匿・完全性保証処理部40をソフトウェアで実現する場合を示す図。

図20は、無線通信制御部20で動作するアプリケーションプログラム46が暗号化プログラム47を呼び出すメカニズムを示す図。

図21は、RLC非透過モードのときのデータ92, 93の具体例を示す図。

図22は、透過データ95, 96の一例として音声データの具体例を示す図。

図23は、透過データ95, 96の一例として非制限デジタルデータの具体例を示す図。

図24は、従来の携帯電話機500を示す図。

発明を実施するための最良の形態

実施の形態1.

図1は、この実施の形態の移動体通信システムの全体構成図である。

無線端末(MS)100は、この発明の無線通信装置の一例である。無線端末(MS)100は、例えば、携帯電話機である。無線端末(MS)100は、無線で無線基地局(BTS)110と接続される。無線基地局(BTS)110は、無線制御局(RNC)120と接続される。無線制御局(RNC)120は、他の無線制御局(RNC)120と

接続される。また、無線制御局（RNC）120は、コアネットワーク（CN）130に接続され、コアネットワーク（CN）130を介して他の無線制御局（RNC）120と接続される。無線基地局（BTS）110と無線制御局（RNC）120とのいずれか又は両方は、無線局とも呼ばれる。

図2は、図1と同じ移動体通信システムの構成図である。特に、無線制御局（RNC）120の内部の構成を示している。

BTS IF部121は、無線基地局（BTS）110を接続する。ハンドオーバ制御部122は、無線基地局（BTS）110間を無線端末（MS）100が移動する場合のハンドオーバを制御する。

対MS信号制御部123は、無線端末（MS）100との間での無線通信制御及びデータの秘匿処理／完全性保証処理を行う。以下に述べる無線端末（MS）100の秘匿処理及び完全性保証処理は、対MS信号制御部123の秘匿処理及び完全性保証処理に対応して行われるものである。即ち、無線端末（MS）100において暗号化されたデータは、対MS信号制御部123において復号化される。逆に、対MS信号制御部123で暗号化されたデータは、無線端末（MS）100において復号化される。また、無線端末（MS）100においてデータの完全性を保証するために付加された認証子は、対MS信号制御部123において検証される。逆に、対MS信号制御部123においてデータの完全性を保証するために付加された認証子は、無線端末（MS）100において検証される。この無線端末（MS）100と対MS信号制御部123におけるデータの秘匿処理及びデータの完全性保証処理は、OSIの7つの階層の内の2番目のレイヤ、即ち、レイヤ2（データリンク層）で行われる。CN IF部124は、コアネットワーク（CN）130とのインタフェースをとる。

RNC IF部125は、他の無線制御局(RNC)120とのインタフェースをとる。対CN信号制御部126は、コアネットワーク(CN)130との間での制御を行う。対RNC信号制御部127は、他の無線制御局(RNC)120との間で制御を行う。制御部128は、無線制御局(RNC)120全体を制御する。スイッチ129は、制御部128の制御に基づいて、無線基地局(BTS)110と無線制御局(RNC)120とコアネットワーク(CN)130との間で制御信号並びにパケットデータをスイッチングする。即ち、スイッチ129は、パケットデータだけでなく、音声等を含む全てのデータをスイッチするとともに、制御信号もスイッチする。

図3は、無線端末(MS)100の構成図である。

無線端末(MS)100は、端末IF部10と無線通信制御部20と無線通信部30と秘匿・完全性保証処理部40を有している。端末IF部10は、カメラ1とビデオ2とB/T(Blue Tooth)3とLCD4とKEY5とLED6とUSIM(Universal Subscriber Identity Module)7とRECEIVER8とMIC9とHSJ(Head Set Jack)0とを接続している。これらのカメラ1からHSJ0は、ユーザ(人間)もしくは接続の対象となる機器とのインターフェースのための処理を行い、ユーザ(人間)もしくは接続の対象となる機器が認識できる情報を入力又は出力するものである。

端末IF部10は、内部に各モジュールIF部11とデータフォーマット変換部12と端末IF制御部13と音声符号化/復号化部14を有している。各モジュールIF部11は、カメラ1からHSJ0との各インタフェースをとる。データフォーマット変換部12は、カメラ1からHSJ0で取り扱う各データフォーマットと無線端末(MS)100内

部で取り扱う各データフォーマットとの間での変換を行う。端末 I F 制御部 1 3 は、端末 I F 部 1 0 の動作を制御する。音声符号化／復号化部 1 4 は、M I C 9 から入力された音声電気信号を音声符号化する。また、音声符号化／復号化部 1 4 は、音声符号化された信号を復号して R E C E I V E R 8 に対して音声電気信号を出力する。

無線通信制御部 2 0 は、無線端末 (M S) 1 0 0 の全体制御を行う。無線通信制御部 2 0 には、C P U、R O M、R A M、ファームウェア等からなるハードウェア回路、或いは、ソフトウェアモジュールが備えられている。無線通信制御部 2 0 は、端末 I F 部 1 0 と無線通信部 3 0 との間でデータを処理するものであり、規格或いはプロトコルにより定められた規則に基づいてデータの変換処理を行う。特に、レイヤ 2 以上の処理を行う。例えば、データの packets 化やデータの連結等を行う。無線通信制御部 2 0 は、レイヤ 2 以上のデータを取り扱うため、データの種別を判断することができる。そして、データの種別に応じて、そのデータが秘匿処理されるべきデータであるか、又は、完全性保証処理されるべきデータであるかを判断することができる。レイヤ 1 のデータでは、データの種別を判断できないため、そのデータが秘匿処理されるべきデータであるか、又は、完全性保証処理されるべきデータであるかを判断することができない。

無線通信部 3 0 は、通信路符号化部 3 1 0 とベースバンド変復調部 3 2 0 と無線部 3 3 0 とアンテナ 3 4 を備えている。通信路符号化部 3 1 0 は、各通信路用の符号化部と復号化部を有している。符号化部として、誤り検出符号化部 3 1 1 と誤り訂正符号化部 3 1 2 と物理フォーマット変換部 3 1 3 を有している。また、復号化部として物理フォーマット変換部 3 1 4、誤り訂正復号化部 3 1 5、誤り検出部 3 1 6 を有している。ベースバンド変復調部 3 2 0 は、帯域の変調及び復調を行う。ベー

スバンド変復調部 3 2 0 は、ベースバンド変調部 3 2 1 とベースバンド復調部 3 2 2 を有している。無線部 3 3 0 は、ベースバンド帯域の信号を伝送帯域に変換もしくは伝送帯域の信号をベースバンド帯域に変換する。無線部 3 3 0 は、アップコンバータ 3 3 1 とダウンコンバータ 3 3 2 を有している。

秘匿・完全性保証処理部 4 0 は、無線通信制御部 2 0 に接続されている。秘匿・完全性保証処理部 4 0 は、無線通信制御部 2 0 からデータを受け取り、秘匿処理を行う。また、データの完全性保証処理を行う。秘匿・完全性保証処理部 4 0 は、無線通信制御部 2 0 から秘匿及び完全性保証処理のための制御信号 9 1 を入力する。また、秘匿・完全性保証処理部 4 0 は、無線通信制御部 2 0 からレイヤ 2 以上の任意の階層における秘匿処理の対象となるデータ及び／又は完全性保証処理の対象となるデータ 9 2 を入力する。秘匿・完全性保証処理部 4 0 は、入力した制御信号 9 1 に基づいてデータ 9 2 に対して秘匿処理及び／又は完全性保証処理を行い、無線通信制御部 2 0 に出力する。制御信号 9 1 の中には、鍵や初期値や秘匿処理と完全性保証処理との選択等のパラメータが含まれている。

図 4 は、秘匿・完全性保証処理部 4 0 の構成図である。

秘匿・完全性保証処理部 4 0 は、I F 部 4 1 0 と 1 つのモジュール 4 1 1 を有している。モジュール 4 1 1 は、秘匿処理と完全性保証処理を 1 つの同一の回路又は 1 つの同一のアルゴリズムで行うものである。秘匿処理を行うか、完全性保証処理を行うかは、制御信号 9 1 により決定される。

ここで、秘匿処理とは、データを暗号化、或いは、復号化することを用いる。また、完全性保証処理とは、データの改竄の有無を検証するために、データに対して認証子を付加する処理、或いは、認証子を再生して

比較することによりデータの改竄の有無を判定する処理のことをいう。

秘匿処理と完全性保証処理は、同一の回路又は同一のアルゴリズム、
或いは、類似の回路又は類似のアルゴリズムを用いて行うことができる
ため、図4に示すように、秘匿処理と完全性保証処理を1つのモジュール
411で行うことが可能である。図4に示す場合は、ハードウェアリ
ソース及びソフトウェアリソースの削減が可能である。以下、モジュール
とは、ハードウェアのみで実現されるもの、ソフトウェアのみで実現
されるもの、ハードウェアとソフトウェアとの組み合わせで実現される
もののいずれかをいうものとする。

ここで、携帯電話機に用いられる秘匿処理と完全性保証処理との具体
例について説明する。

図14は、ARIB STD-T63 33.102, 3G Security; Security Architecture, Section 6.3. に示された図である。

図15は、ARIB STD-T63 33.102, 3G Security; Security Architecture, Figure 16b. に示された図である。

図16は、ARIB STD-T63 33.102, 3G Security; Security Architecture, Figure 16. に示された図である。

図14は、無線回線上での暗号化方法を示している。図14において
、記号の意味は、以下の通りである。

CK: cipher key (暗号鍵)

F8: データ秘匿用関数

IK: integrity key (メッセージ認証鍵)

F9: データ完全性用関数

携帯電話事業者は、 $f_1 \sim f_5$ という関数を使い、認証処理を実現している。この処理の中で生成したCKとIKと呼ぶ128ビットの暗号鍵を、データ秘匿用関数(f_8)とデータ完全性用関数(f_9)に渡している。

- 5 図15は、無線回線上での暗号化方法を示している。図15において、記号の意味は、以下の通りである。

f_8 : データ秘匿用関数

CK : cipher key (暗号鍵)

- MESSAGE : ユーザー・データ及び信号情報など送信者が受信者
10 に送りたい暗号化前の平文

COUNT-C : 送受信の通算回数を示す数値データ。送受信のたびに1を加算する。

BEARER : 論理チャネルを識別するためのビット

DIRECTION : 暗号文の送信方向を区別するためのビット

- 15 LENGTH : MESSAGE或いは暗号文のビット長

図15に示すように、データ秘匿用関数 f_8 で作成した乱数列を基にデータ暗号化／復号化を行う。

図16は、メッセージ認証子生成方法を示している。図16において、記号の意味は、以下の通りである。

- 20 f_9 : データ完全性用関数

IK : integrity key (メッセージ認証鍵)

COUNT-I : 送受信の通算回数を示す数値データ。送受信のたびに1を加算する。

- MESSAGE : ユーザー・データ及び信号情報など送信者が受信者
25 に送りたい暗号化前の平文

DIRECTION : 暗号文の送信方向を区別するためのビット

FRESH : ユーザー毎に生成する乱数

MAC-I : message authentication code for integrity (送信者が計算するメッセージ認証子)

- 5 XMAC-I : expected message authentication code for integrity (受信者が計算するメッセージ認証子)

図16に示すように、受信者側で2つのメッセージ認証子を比較することによりデータの完全性がチェックできる。

- 10 次に、動作について説明する。

無線網内で端末とネットワーク間の暗号化通信を行うには、データをやり取りする前に二者間で一方が相手を正当であると、或いは、双方が通信相手として正当であると確認する認証 (authentication) という処理が必要になる。

- 15 図14に示すように、一連の認証処理で端末とネットワークの双方は、関数 $f_1 \sim f_5$ と呼ぶ5つの関数を使う。この関数は、認証と並行して端末とネットワークの両方に、それぞれ128ビットの暗号鍵 ($CK = cipher\ key$) とメッセージ認証鍵 ($IK = integrity\ key$) を生成する。

- 20 これら2つの鍵は、相互に認証した端末とネットワークだけが同じものを持つことができ、後述する f_8 と f_9 との2つの関数で使われる。これら2つの鍵は通信毎に異なり、しかもそれらの間の規則性がない。そして、通信が終了した時点で廃棄される。

- 25 なお、この認証に必要な処理のメカニズム (プロトコル) は、標準化されているが、認証処理で用いられる $f_1 \sim f_5$ の関数は標準化されておらず、オペレータが独自に決めることになっている。

認証処理が完了した後は、秘匿処理に用いられるデータ秘匿 (data confidentiality) 技術と完全性保証処理に用いられるデータ完全性 (data integrity) 技術で、データのセキュリティを保っている。

- 5 1つ目のデータ秘匿技術は、無線ネットワーク上で音声を含むユーザー・データや信号情報を暗号化し、盗聴を防止する技術である。このデータ秘匿を実現するために、データ秘匿用関数 (以下、 f_8 と呼ぶ) という関数を用いる。

- 10 図 15 に示すデータを秘匿してやり取りする場合、送信者は認証の際に生成した暗号鍵 (CK) を使う。更に、 f_8 には、CK の他に、暗号化／復号化対象データのビット長 (LENGTH)、アップ／ダウンリンク (DIRECTION)、カウンタ (COUNT-C)、論理チャネル識別子 (BEARER) を入力することで乱数列が生成される。

- 15 ここで、アップ／ダウンリンクとは、暗号文が端末から基地局へ送信されるのか、或いは、基地局から端末へ送信されるのかを区別するビットをいう。また、カウンタとは、送受信の通算回数を示すデータである。カウンタには、送受信のたびに決められた値を加算する。カウンタは、過去に送られた暗号文を後に送りつける攻撃を防ぐために用いられる。また、論理チャネルの識別子とは、暗号化を行う論理チャネルを識別
20 するビットのことである。

生成した乱数列と暗号化したいデータ／信号情報との排他的論理和をとって暗号文を生成し、受信者に送信する。

- CK 以外のパラメータは、送信者から暗号化せずに受信者へ送付する。但し、CK だけは認証処理の過程で受信者側でも同じものが生成され
25 ているため、送信する必要がない。

CK 以外のパラメータが第三者に渡ったとしても、CK が秘密であれ

ば暗号文を解読するための乱数列が生成できないため、元のメッセージの安全性は保たれる。

受信者側は、送られてきたパラメータと予め持っていたCKを使って乱数列を生成し、送られてきた暗号文と排他的論理和をとって、元のメッセージを復号する。

これは、ISO/IEC 10116で定義されたブロック暗号の利用モードの1つであるOFB (output feedback) モードの変形である。OFBモードは、暗号文に伝送路上で発生したノイズが混入しても、復号時点でそのノイズ部分を拡大することがないため、特に無線音声通信で採用される場合が多い。

2つ目のデータ完全性技術は、無線回線上の信号情報にメッセージ認証子（完全性認証子）を付加することで信号の情報の改竄の有無を検出する技術である。メッセージ認証技術とも呼ばれている。このデータ完全性をを実現するために、データ完全性関数（以下、f9と呼ぶ）を用いる。このf9のコア部分にもF8と同じ暗号アルゴリズムが用いられている。

まず、認証の際にメッセージ認証鍵生成関数f4を使ってメッセージ認証鍵（IK）を生成し、f9に渡す。図16に示すように、f9にメッセージ認証鍵の他、データ（MESSAGE）、アップ/ダウンリンク（DIRECTION）、カウンタ（COUNT-C）、ユーザー毎に生成する乱数（FRESH）を入力すると、メッセージ認証子（MAC-I又はXMAC-I）が生成される。

これらのパラメータも送信者から暗号化されないデータ・フォーマットのエリアに乗せて受信者へ送付される。これらのパラメータが第三者に渡っても、メッセージ認証鍵（IK）が秘密であれば、安全性は保たれるのはデータの秘匿の場合と同じである。

送信者は、このメッセージ認証子（MAC-I）をデータに付加して、受信者へ送信する。受信者は同様に、f9を使ってメッセージ認証子（XMAC-I）を計算する。MAC-IとXMAC-Iを比較し、同じであれば、改竄がなかったことを確認できる。

5 なお、改竄ありと検出された場合の処理の一例として、

（１）相手に再送信を要求し、再度受信したメッセージ認証子が正当かを確認する。

（２）続けて何回か改竄ありと検出した場合は、接続を切断するなどの対応をとる。

10 3Gpp仕様（詳細は、http://www.3gpp.org/About_3GPP/3gpp.htmを参照のこと）によると、暗号化／復号化モジュールは、図15のように、入力された平文（暗号化されるデータ）を暗号文（暗号化されたデータ）に暗号化し出力する機能、また、暗号文を平文に復号化し出力する機能を持つ。3Gpp仕様
15 に基づくとする、図3の制御信号91の具体例は、上記COUNT／BERARER／DIRECTION／CK／LENGTHが該当する。

また、図3のデータ92、93の具体例としては、例えば、図21に示すように、「MACSDU」又は「RLCPDU（datapart）」となる。ここで、「RLCPDU（datapart）」とは、RLCPDUの上位1Octもしくは2Oct（1バイトもしくは2バイト）を削除した部分（図21の「DATA FOR CIPHERING」の部分）となる。「MACSDU」又は「RLCPDU（datapart）」は、図15のMESSAGEの一例である。また、MAC
20 SDUは、Media Access Control Service
25 Data Unitのことである。RLCPDUは、Radio

Link Control Protocol Data Unitのことである。メッセージフローの各メッセージは、RLCPDUから、RLCヘッダ削除後、レイヤ3において組み立てられたものとなる。

RLCPDUにおいて、1Octもしくは2Octの秘匿対象外部分
5 が存在するが、RLCPDU全てを秘匿・完全性保証処理部40に入力し、秘匿・完全性保証処理部40にて、1Octもしくは2Oct秘匿を行わないようにしている。その理由は、秘匿処理を行う全てのデータ単位(RLCPDU)から1Octもしくは2Octの秘匿対象外部分を取り除くため、1Octもしくは2Octのシフト処理を無線通信制
10 御部20において実行させることにより発生する無線通信制御部20の負荷を低減するためである。

図5は、秘匿・完全性保証処理部40の他の例を示す図である。

図5において特徴となる点は、秘匿処理部420と完全性保証処理部430を個別に設けた点である。秘匿処理部420の内部には、暗号化
15 /復号化部421が設けられている。完全性保証処理部430の内部には、完全性認証子付加/完全性確認部431が設けられている。暗号化/復号化部421は、暗号化と復号化を1つの同一モジュールを用いて行う場合を示している。完全性認証子付加/完全性確認部431は、完全性認証子の付加と完全性の確認を1つの同一のモジュールで行う場合
20 を示している。図5に示す場合は、暗号化と復号化が同じ関数であった場合及び完全性認証子付加と完全確認が同じ関数であった場合に、取り得る構成である。図5に示す場合は、図6に示す場合に比べ、ハードウェアリソース及びソフトウェアリソースの削減が可能である。

図6は、秘匿・完全性保証処理部40の他の構成を示す図である。

25 図6の特徴は、秘匿処理部420において、暗号化部422と復号化部423を個別に設けた点である。また、完全性保証処理部430にお

いて、完全性認証子付加部 4 3 2 と完全性確認部 4 3 3 を個別に設けた点である。図 6 に示す場合は、暗号化と復号化が同じ又は違う関数であった場合及び完全性認証子付加と完全性確認が同じ又は違う関数であった場合を取る構成である。図 6 の場合は、暗号化、復号化、完全性認証子付加、完全性確認を個別に実行でき、送受信されるデータが同時並列に秘匿処理、或いは、完全性保証処理されるので、処理の高速化が可能である。

図 7 は、秘匿処理部 4 2 0 において、複数の暗号化部 4 2 2 と複数の復号化部 4 2 3 を設けた場合を示している。また、完全性保証処理部 4 3 0 において、複数の完全性認証子付加部 4 3 2 と複数の完全性確認部 4 3 3 を設けた場合を示している。無線端末 (MS) 1 0 0 が動作している場合に、複数のチャネルが同時に処理されなければならない場合がある。例えば、音声とファクシミリデータの 2 種類のデータが同時に伝送されるような場合には、少なくとも 2 チャネルのデータが同時に処理される必要がある。このような場合には、音声データを暗号化部 1 で暗号化し、ファクシミリデータを暗号化部 2 で暗号化することができる。また、復号する場合にも、同時に複数チャネルのデータを復号化することができる。暗号化部 4 2 2 と復号化部 4 2 3 と完全性認証子付加部 4 3 2 と完全性確認部 4 3 3 の数 (図 7 では、 n 個) は、全て同一である必要はなく、無線端末 (MS) 1 0 0 において同時に処理すべきチャネルの数に応じて各部分の数を決定すればよい。或いは、各チャネルに対応するのではなく、ある 1 つのチャネルに大量データの高速処理を行う必要が生じた場合に、その 1 つのチャネルに割り当てられた大量データを 2 つの暗号化部により処理するようにしても構わない。即ち、暗号化部 4 2 2 と復号化部 4 2 3 と完全性認証子付加部 4 3 2 と完全性確認部 4 3 3 の各部の数は、同時に処理すべきチャネルの数及び/又はデータ

量により決定すればよい。

また、暗号化部 4 2 2 の最大数と復号化部 4 2 3 の最大数は異なってもよい。

また、完全性認証子付加部 4 3 2 の最大数と完全性確認部 4 3 3 の最大数は異なってもよい。

図 8 は、秘匿処理部 4 2 0 に複数の暗号化／復号化部 4 2 1 を設けた場合を示している。また、完全性保証処理部 4 3 0 に複数の完全性認証子付加／完全性確認部 4 3 1 を設けた場合を示している。

図 8 は、図 5 に示す暗号化／復号化部 4 2 1 と完全性認証子付加／完全性確認部 4 3 1 を複数にしたものである。図 8 に示す場合は、暗号化と復号化が同じ関数であった場合に、複数のチャネルに対応して複数の暗号化／復号化部 4 2 1 を設けた場合を示している。同様に、完全性認証子付加と完全性確認が同じ関数であった場合に、複数のチャネルに対応して完全性認証子付加／完全性確認部 4 3 1 を複数設けた場合を示している。図 8 の場合は、図 7 の場合に比べて、ハードウェアリソース及びソフトウェアリソースの削減を行うことが可能である。

図 4 から図 8 においては、秘匿・完全性保証処理部 4 0 が秘匿処理部 4 2 0 と完全性保証処理部 4 3 0 とを両方備えている場合を示したが、秘匿・完全性保証処理部 4 0 が秘匿処理部 4 2 0 又は完全性保証処理部 4 3 0 のいずれか片方だけ備えている場合でもよい。秘匿・完全性保証処理部 4 0 が秘匿処理部 4 2 0 又は完全性保証処理部 4 3 0 の一方だけ備えている場合は、他方の処理は、無線通信制御部 2 0 が行えばよい。実施の形態 2.

図 9 は、無線端末 (MS) 1 0 0 の他の例を示す構成図である。

図 9 が図 3 と異なる点は、端末 I F 部 1 0 と秘匿・完全性保証処理部 4 0 との間でデータの入出力が行われる点である。また、無線通信部 3

0と秘匿・完全性保証処理部40との間でデータの入出力が行われる点である。図9において、非透過データ97は、パケットデータ等の非透過データである。また、透過データ95, 96は、音声データや非制限デジタルデータ等の透過データである。透過データとは、OSIで定義されているあるレイヤ、或いは、あるレイヤのサブレイヤにおいて、入力から出力まで、そのデータが一切変更されないデータをいう。一方、非透過データとは、あるレイヤ、或いは、あるレイヤのサブレイヤにおいて、入力から出力まで、そのデータのフォーマット変換処理等の何等かのデータ処理が必要なデータをいう。例えば、レイヤ2のRLC (Radio Link Control) サブレイヤにおいて、SDU (Service Data Unit) とPDU (Protocol Data Unit) とが異なる場合は、そのデータは非透過データであり、レイヤ2のMAC (Media Access Control) サブレイヤにおいて、SDUとPDUが同一の場合、そのデータは透過データである。図9に示す場合は、無線通信部30との間で入出力されるレイヤ1のデータに対して何等処理を行うことなく、端末IF部10に引き渡すことができるデータ、例えば、音声データを、透過データとしている。一方、無線通信部30から出力されるレイヤ1のデータに対して何等かの処理を行わなければならないデータ、例えば、パケットデータを、非透過データとしている。

図9の透過データ95, 96の具体例は、前述した通り、音声データや非制限デジタルデータであるが、それぞれのデータは、レイヤ1とレイヤ2の間に定義される単位 (Transport Block) に分割されたものであり、これらTransport Blockに分割されたデータは透過データであるため、前述の通り、MAC PDU (かつ、MAC SDU) と等価であるため、Transport Block

に分割されたデータそれぞれが、秘匿の単位と同一となる。

また、音声データ等は、ユーザーデータであり、ユーザーデータは、RLCサブレイヤにおいても透過データであることから、この伝送形態をシリアルインタフェースとして、ARIB規定のMT (Mobile Terminal) - TA (Terminal Adaptor) I/F (図22, 図23) とすると、MT-TA I/Fのシリアルフォーマットに対しそのまま、秘匿を施すことが可能な伝送形態となる。

また、図9の非透過データ97の具体例は、前述した通り、パケットデータやシグナリングのためのデータであるが、各データは、レイヤ1とレイヤ2との間に定義される単位 (Transport Block) に分割されたものである。

図9に示す秘匿・完全性保証処理部40は、無線通信制御部20との間で非透過データに対して秘匿処理と完全性保証処理を選択的に行うとともに、端末IF部10と無線通信部30との間で入出力される透過データに対して、例えば、秘匿処理を必ず行うものである。秘匿・完全性保証処理部40は、透過データに対しては完全性保証処理を行わない。もし、透過データのなかに秘匿処理を行いたくないものがある場合には、無線通信制御部20は、その秘匿処理を行いたくない透過データを秘匿・完全性保証処理部40に入力させず無線通信制御部20に入力させればよい。或いは、その秘匿処理を行いたくない透過データを秘匿・完全性保証処理部40に入力させるが、無線通信制御部20からの制御信号を用いてその透過データに秘匿処理を行わせないようにしてもよい。

図10は、秘匿・完全性保証処理部40の構成図である。

図10において、図5と異なる点は、新たに秘匿処理部460が設けられた点である。秘匿処理部460には、暗号化部462と復号化部463が設けられている。暗号化部462は、端末IF部10からの透過

データ 9 5 を入力し、入力したデータを暗号化し、透過データ 9 6 とし
て無線通信部 3 0 へ出力する。一方、復号化部 4 6 3 は、無線通信部 3
0 から透過データ 9 6 を入力し、復号化し、透過データ 9 5 として端末
I F 部 1 0 へ出力する。秘匿処理部 4 6 0 のこれらの処理は、I F 部 4
5 1 0 からの制御信号 9 9 に基づいて行われる。制御信号 9 9 は、制御信
号 9 1 から生成された制御信号である。従って、秘匿処理部 4 6 0 は、
無線通信制御部 2 0 からの制御信号に基づいて秘匿処理を行うことにな
る。図 1 0 において、データ 9 2 は、バスを介したパラレルインタフェ
ースを用いて入出力される。一方、透過データ 9 5 と 9 6 は、シリアル
10 インタフェースを介して秘匿処理部 4 6 0 に対して入出力される。この
ように、図 1 0 は、秘匿・完全性保証処理部 4 0 がパラレルインタフェ
ースとシリアルインタフェースの 2 系統の入出力インタフェースを備え
ている場合を示している。

図 1 1 は、図 7 に示した秘匿・完全性保証処理部 4 0 の構成に秘匿処
15 理部 4 6 0 を付加した場合を示している。図 1 1 に示すような秘匿処理
部 4 6 0 の構成は、図 1 2 に示すように、暗号化部又は復号化部がキー
ストリームを発生させ、シリアルデータと排他的論理和をとる場合に有
効な構成である。

図 1 1 は、透過データ 9 5, 9 6 がシリアルインタフェースを介して
20 秘匿処理部 4 6 0 に入出力される場合であって、かつ、そのシリアルイ
ンタフェースを介して入出力されるシリアルデータに、複数チャネルの
データが多重化されている場合を示している。例えば、チャネル 1 のデ
ータの次にチャネル 2 のデータがシリアルデータとして入力された場合
、チャネル 1 に対応する暗号化部 1 からキーストリームを発生させデー
25 タ多重部 4 8 1 へ出力し、チャネル 2 に対応する暗号化部 2 からキー
ストリームを発生させデータ多重部 4 8 1 へ出力し、データ多重部 4 8 1

において、これらのキーストリームを入力されるデータ 9 5 のデータ系列と同じフォーマットに多重する。この多重したキーストリームと入力されるデータ 9 5 のデータ系列との排他的論理和を排他的論理和回路 4 8 3 により演算する。秘匿処理部 4 6 0 のこれらの動作は制御信号 9 9 5 に基づいて、即ち、無線通信制御部 2 0 から送られてきた制御信号 9 1 に基づいて行われる。図 1 1 の構成によれば、シリアルデータの遅延が排他的論理和回路 4 8 3 の演算のみで済み、高速な処理を行うことが可能である。

図 1 3 は、図 1 0 の秘匿処理部 4 2 0 と秘匿処理部 4 6 0 とをあわせて 1 つの秘匿処理部 4 7 0 とした場合を示している。

秘匿処理部 4 7 0 は、パラレルインタフェースから入出力されるデータ 9 2 とシリアルインタフェースから入出力されるデータ 9 5 , 9 6 の両方を処理する。秘匿処理部 4 7 0 は、秘匿処理部 4 2 0 と秘匿処理部 4 6 0 を 1 つにまとめたものであるため、ハードウェアリソースの削減 15 が可能である。秘匿処理部 4 7 0 における透過データと非透過データの処理動作のスイッチングは、制御信号 9 9 、即ち、無線通信制御部 2 0 から出力された制御信号 9 1 に基づいて行われる。

前述した秘匿・完全性保証処理部 4 0 は、ハードウェアで構成することができる。例えば、FPGA やカスタム LSI で実現することができる。また、秘匿・完全性保証処理部 4 0 は、ソフトウェアプログラムで 20 実現することもできる。秘匿・完全性保証処理部 4 0 がソフトウェアプログラムで実現される場合、ソフトウェアプログラムは無線通信制御部 2 0 にある CPU により実行されることになる。

また、秘匿・完全性保証処理部 4 0 は、ハードウェアとソフトウェア 25 の組み合わせにより実現することができる。例えば、DSP (Digital Signal Processor) とその DSP により実行

されるマイクロプログラムやファームウェアプログラムにより実現することができる。

以下、図 17 から図 20 を用いて、具体例を説明する。

図 17 は、暗号化／復号化部 421 の中で用いられる暗号化モジュール 51（又は復号化モジュール 71）の構成図である。

暗号化モジュール 51 は、鍵スケジュール部 511 とデータランダムライズ部 512 を有している。鍵スケジュール部 511 は、1 つの鍵 K を入力して n 個の拡大鍵 $Ext K_1 \sim Ext K_n$ を生成する。データランダムライズ部 512 は、関数 F と XOR 回路とにより乱数を発生させる。

関数 F は、拡大鍵を入力して非線形データ変換を行う。

暗号モジュール 51 においては、例えば、

- (1) DES (Data Encryption Standard)、又は、
- (2) 国際公開番号 WO 97/9705 (米国特許出願番号 08/83640) に開示されたブロック暗号アルゴリズムである MISTY、又は、
- (3) 上記ブロック暗号アルゴリズム MISTY をベースとした 64 ビットブロック暗号であり、次世代携帯電話用国際標準暗号 (IMT 2000) として採用されることが決定されたブロック暗号アルゴリズムである KASUMI、又は、

- (4) 日本特許出願番号 2000-64614 (出願日 2000 年 3 月 9 日) に記載されたブロック暗号アルゴリズムである Camellia などのブロック暗号アルゴリズムを用いることができる。また、復号モジュール 71 においても、DES、MISTY、KASUMI 又は Camellia などのブロック暗号アルゴリズムを用いることができる。

図 18 は、前述した秘匿・完全性保証処理部 40 の実装形式を示す図である。

図 18 は、FPGA 又は IC 又は LSI の中に前述した秘匿・完全性保証処理部 40 が実現されている場合を示している。即ち、前述した秘匿・完全性保証処理部 40 は、ハードウェアで実現することができる。また、図示していないが、プリントサーキットボードにより実現することも可能である。

図 19 は、前述した秘匿・完全性保証処理部 40 をソフトウェアで実現する場合を示している。

10 前述した秘匿・完全性保証処理部 40 は、暗号化プログラム 47 で実現することができる。暗号化プログラム 47 は、ROM (Read Only Memory) 42 (記録媒体の一例) に記憶されている。暗号化プログラム 47 は、RAM (Random Access Memory) 又はフレキシブルディスク又は固定ディスク等の他の記録媒体
15 に記録されていてもよい。また、暗号化プログラム 47 は、サーバコンピュータからダウンロードされてもよい。暗号化プログラム 47 は、サブルーチンとして機能する。暗号化プログラム 47 は、RAM 45 に記憶されたアプリケーションプログラム 46 からサブルーチンコールにより呼び出されて実行される。或いは、暗号化プログラム 47 は、割り込み制御部 43 で受け付ける割り込みの発生により起動されるようにしても構わない。メモリ 55 は、RAM 45 の一部であっても構わない。アプリケーションプログラム 46、暗号化プログラム 47 は、CPU 41
20 により実行されるプログラムである。

図 20 は、無線通信制御部 20 で動作するアプリケーションプログラム 46 が暗号化プログラム 47 を呼び出すメカニズムを示している。

アプリケーションプログラム 46 は、鍵 K とイニシャルバリュー IV

と平文Mと暗号文Cをパラメータにして暗号化プログラム47を呼び出す。暗号化プログラム47は、鍵KとイニシャルバリューIVと平文Mを入力し、暗号文Cを返すものである。暗号化プログラム47と復号プログラムが同一のときは、鍵KとイニシャルバリューIVと暗号文Cと
5 平文Mをパラメータにして暗号化プログラム47を呼び出す。

また、図示しないが、暗号化プログラム47は、デジタルシグナルプロセッサと、そのデジタルシグナルプロセッサにより読み込まれて実行されるプログラムによって実現しても構わない。即ち、ハードウェアとソフトウェアの組み合わせによって暗号化プログラム47を実現しても
10 構わない。

図18、図19、図20は、主として、暗号化の場合を説明したが、復号化でも同様の方式で実現できる。

図18及び図19に示したような暗号化形態及び復号化形態は、電子機器に対してインストールすることができる。例えば、パーソナルコンピュータやファクシミリ装置や携帯電話やビデオカメラやデジタルカメラやテレビカメラ等のあらゆる電子機器にインストールすることができる。特に、この実施の形態における特徴が発揮できるのは、複数のチャネルからのデータを暗号化復号化する場合に有効である。或いは、複数のユーザからのデータがアットランダムに到着して復号化する場合に、
15 或いは、複数のユーザに対するデータがアットランダムに発生して、それぞれのデータをリアルタイムに暗号化するような場合に有効である。即ち、暗号化復号化するデータの数に比べて暗号化復号化する装置の数が少ない場合に、前述した実施の形態の暗号化、復号化が非常に有効である。例えば、多くのクライアントコンピュータをサポートしなければならないサーバコンピュータや多くの携帯電話機からのデータを集配しなければならない基地局や回線コントローラなどに、前述した暗号化方
20
25

式や復号化方式が非常に有効である。

また、前述した例においては、無線通信制御部 20 と秘匿・完全性保証処理部 40 がバスを介したパラレルインタフェースでつながれている場合を示したが、シリアルインタフェースを用いても構わない。また、
5 端末 I/F 部 10 と秘匿・完全性保証処理部 40 及び無線通信部 30 と秘匿・完全性保証処理部 40 がシリアルインタフェースで接続される場合を示したが、より高速な処理を行うためには、シリアルインタフェースではなく、パラレルインタフェースを用いても構わない。

また、図 9，図 10 においては、秘匿処理部 460 を秘匿・完全性保証
10 証処理部 40 の内部に設ける場合を示したが、秘匿処理部 460 を秘匿・完全性保証処理部 40 から外部に独立させて、秘匿処理部 460 を端末 I/F 部 10 と無線通信部 30 との間に設けてもよい。

産業上の利用可能性

15 以上のように、前述した実施の形態によれば、レイヤ 1（物理層）において秘匿処理を行わないように、レイヤ 2 以上の階層において秘匿処理及び完全性保証処理を行うようにしたので、データの種別に応じて秘匿処理の可否及び完全性保証処理の可否を決定することができる。

例えば、透過データに対しては秘匿処理のみを行い、非透過データに
20 対して秘匿処理と完全性保証処理の両方を行うことが可能になる。或いは、非透過データであっても秘匿処理と完全性保証処理とをそれぞれ行ったり、行わなかったり選択することが可能になる。

また、上記実施の形態によれば、秘匿・完全性保証処理部の内部にチャンネルの数やデータ量に応じて複数の秘匿処理部と複数の完全性保証処
25 理部を設けているので、同時並列処理による高速データ処理が可能となる。

請求の範囲

1. データを入力する端末インタフェース部と、
端末インタフェース部が入力したデータを入力し、プロトコルに基づ
5 いてデータを処理して出力する無線通信制御部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号
に基づいて、入力したデータに対して少なくともデータを暗号化する秘
匿処理とデータの改竄を検出するための完全性認証子を生成する完全性
保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部
10 へ出力する秘匿・完全性保証処理部と、

無線通信制御部から出力されたデータを入力して変調し送信する無線
通信部と
を備えたことを特徴とする無線通信装置。

2. 上記秘匿・完全性保証処理部は、
15 無線通信制御部から制御信号を入力し、入力した制御信号に基づいて
端末インタフェース部からデータを選択的に入力するとともに、
入力したデータに対して秘匿処理を行い、
秘匿処理したデータを無線通信部に出力することを特徴とする請求項
1 記載の無線通信装置。

20 3. 上記端末インタフェース部は、透過データと非透過デー
タとを出力し、

上記無線通信制御部は、非透過データを端末インタフェース部から入
力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとと
もに、透過データを端末インタフェース部から秘匿・完全性保証処理部
25 に入力させて秘匿処理させることを特徴とする請求項 2 記載の無線通信
装置。

4. 上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする請求項1記載の無線通信装置。

5. 上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする請求項2記載の無線通信装置。

6. 上記秘匿・完全性保証処理部は、
入力したデータを暗号化する暗号化部を有する秘匿処理部と、
10 入力したデータに対して完全性認証子を付加する完全性認証子付加部を有する完全性保証処理部と
を備えたことを特徴とする請求項1記載の無線通信装置。

7. 上記秘匿処理部は、複数の暗号化部を有することを特徴とする請求項6記載の無線通信装置。

15 8. 上記完全性保証処理部は、複数の完全性認証子付加部を有することを特徴とする請求項6記載の無線通信装置。

9. 上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する1つのモジュールであり、その1つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部のいずれかの処理
20 を実行することを特徴とする請求項6記載の無線通信装置。

10. データを受信して復調する無線通信部と、
無線通信部により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御部と、
25 無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘

匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

5 無線通信制御部により処理されたデータを入力して出力する端末インタフェース部と
を備えたことを特徴とする無線通信装置。

1 1. 上記秘匿・完全性保証処理部は、
無線通信制御部から制御信号を入力し、入力した制御信号に基づいて無線通信部からデータを選択的に入力するとともに、
10 入力したデータに対して秘匿処理を行い、
秘匿処理したデータを端末インタフェース部に出力することを特徴とする請求項 1 0 記載の無線通信装置。

1 2. 上記無線通信部は、透過データと非透過データとを出力し、
15 上記無線通信制御部は、非透過データを無線通信部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを無線通信部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする請求項 1 1 記載の無線通信装置。

1 3. 上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする請求項 1 0 記載の無線通信装置。

1 4. 上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする請求項 1 1 記載の無線通信装置。
25

1 5. 上記秘匿・完全性保証処理部は、

入力したデータを復号化する復号化部を有する秘匿処理部と、
入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部を有する完全性保証処理部とを備えたことを特徴とする請求項 10 記載の無線通信装置。

5 16. 上記秘匿処理部は、複数の復号化部を有することを特徴とする請求項 15 記載の無線通信装置。

 17. 上記完全性保証処理部は、複数の完全性確認部を有することを特徴とする請求項 15 記載の無線通信装置。

10 18. 上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する 1 つのモジュールであり、その 1 つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行することを特徴とする請求項 15 記載の無線通信装置。

 19. データを無線通信する無線通信装置において、
15 データを入出力する端末インタフェース部と、
 プロトコルに基づいてデータの処理をする無線通信制御部と、
 データを無線通信する無線通信部と、
 端末インタフェース部と無線通信制御部と無線通信部との三者間に設けられ、無線通信制御部との間でデータに対して少なくともデータを暗
20 号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース部から無線通信部へのデータを暗号化するとともに無線通信部から端末インタフェース部へのデータを復号する秘匿・完全性保証処理部とを備えたことを特徴とする無線通信装置。

25 20. 上記秘匿・完全性保証処理部は、
 入力したデータに対して秘匿処理を行う秘匿処理部と、

入力したデータに対して完全性保証処理を行う完全性保証処理部とを個別に備えたことを特徴とする請求項 19 記載の無線通信装置。

21. 上記秘匿処理部は、

5 端末インタフェース部から無線通信部へのデータを暗号化する暗号化部と、

無線通信部から端末インタフェース部へのデータを復号化する復号化部とを個別に有することを特徴とする請求項 19 記載の無線通信装置。

22. 上記完全性保証処理部は、

10 入力したデータに対して完全性保証処理を行う完全性認証子を付加する完全性認証子付加部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部とを個別に有することを特徴とする請求項 19 記載の無線通信装置。

15 23. 上記通信装置は、携帯型移動電話機であることを特徴とする請求項 19 記載の無線通信装置。

24. 上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする請求項 6 記載の無線通信装置。

20 25. 上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする請求項 15 記載の無線通信装置。

26. 上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする請求項 20 記載の無線通信装置。

25 27. 上記無線通信装置は、携帯電話機であることを特徴とする請求項 1 記載の無線通信装置。

28. 上記無線通信装置は、携帯電話機であることを特徴とする請求項10記載の無線通信装置。

29. 上記無線通信装置は、携帯電話機であることを特徴とする請求項19記載の無線通信装置。

5 30. 上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする請求項1記載の無線通信装置。

31. 上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする請求項10記載の無線通信装置。

10 32. 上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする請求項19記載の無線通信装置。

33. 上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする請求項30記載の無線通信装置。

34. 上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする請求項31記載の無線通信装置。

15 35. 上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする請求項32記載の無線通信装置。

36. データを入力する端末インタフェース工程と、
端末インタフェース工程が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

20 無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

25 無線通信制御工程から出力されたデータを入力して変調し送信する無線通信工程と

を備えたことを特徴とする無線通信方法。

37. データを受信して復調する無線通信工程と、

無線通信工程により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

- 5 無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

- 10 無線通信制御工程により処理されたデータを入力して出力する端末インタフェース工程と

を備えたことを特徴とする無線通信方法。

38. データを無線通信する無線通信方法において、

データを入出力する端末インタフェース工程と、

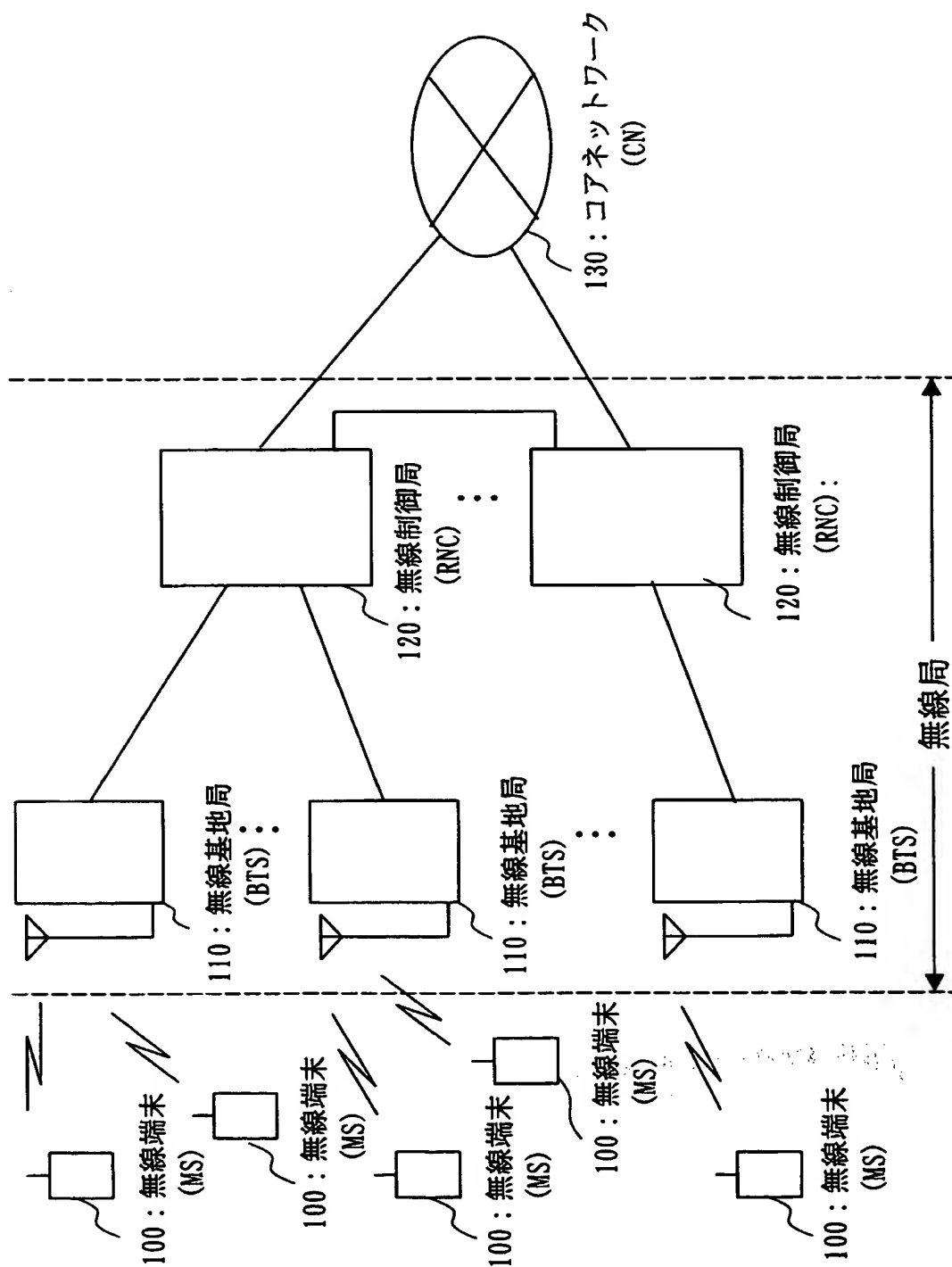
- 15 プロトコルに基づいてデータの処理をする無線通信制御工程と、
データを無線通信する無線通信工程と、

- 端末インタフェース工程と無線通信制御工程と無線通信工程との三者間に設けられ、無線通信制御工程との間でデータに対して少なくともデータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース工程から無線通信工程へのデータを暗号化するとともに無線通信工程から端末インタフェース工程へのデータを復号する秘匿・完全性保証処理工程と
- 20 を備えたことを特徴とする無線通信方法。

THIS PAGE BLANK (USPTO)

1 / 24

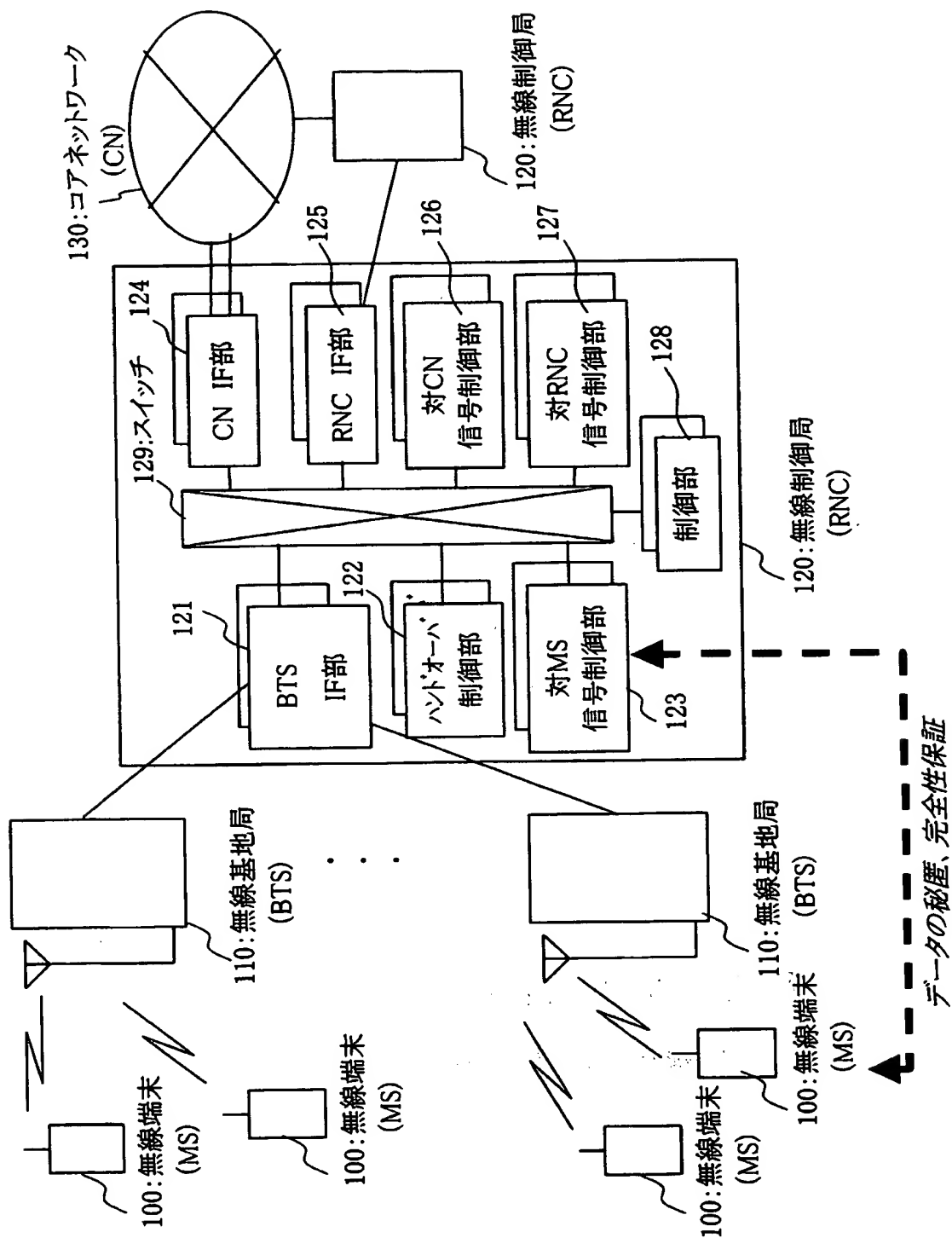
図 1



THIS PAGE BLANK (USPTO)

2 / 24

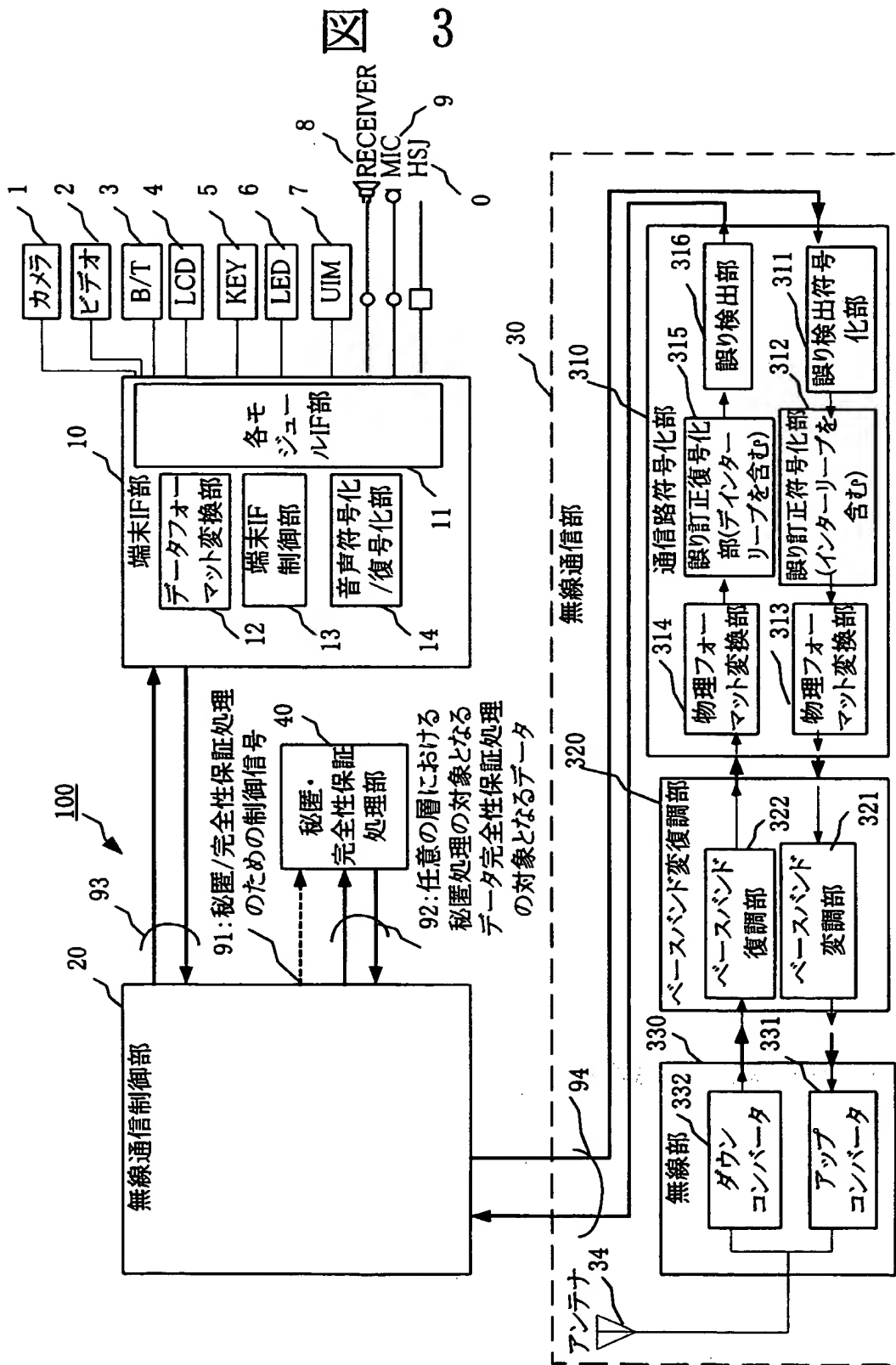
図 2



THIS PAGE BLANK (USPTO)

3 / 24

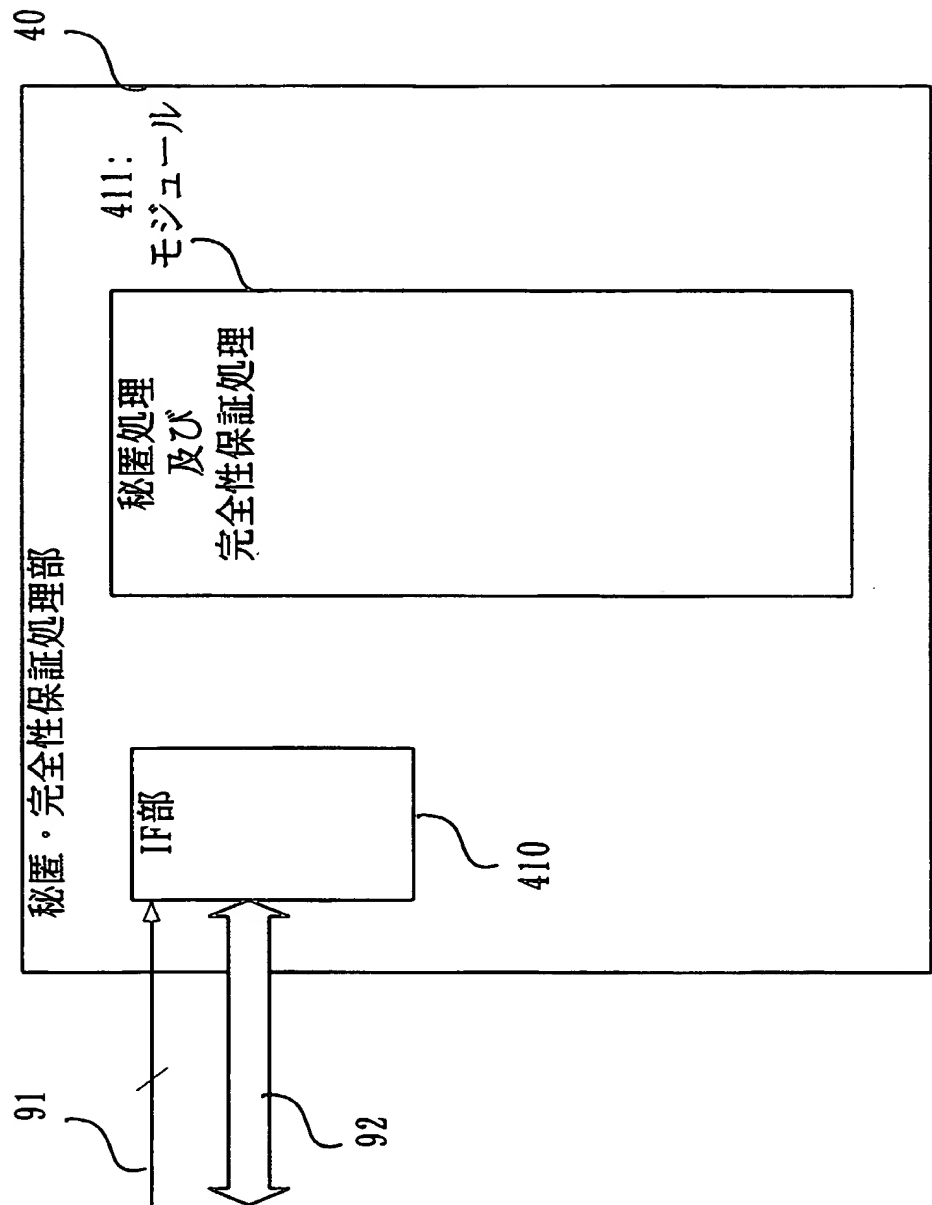
3



THIS PAGE BLANK (USPTO)

4 / 24

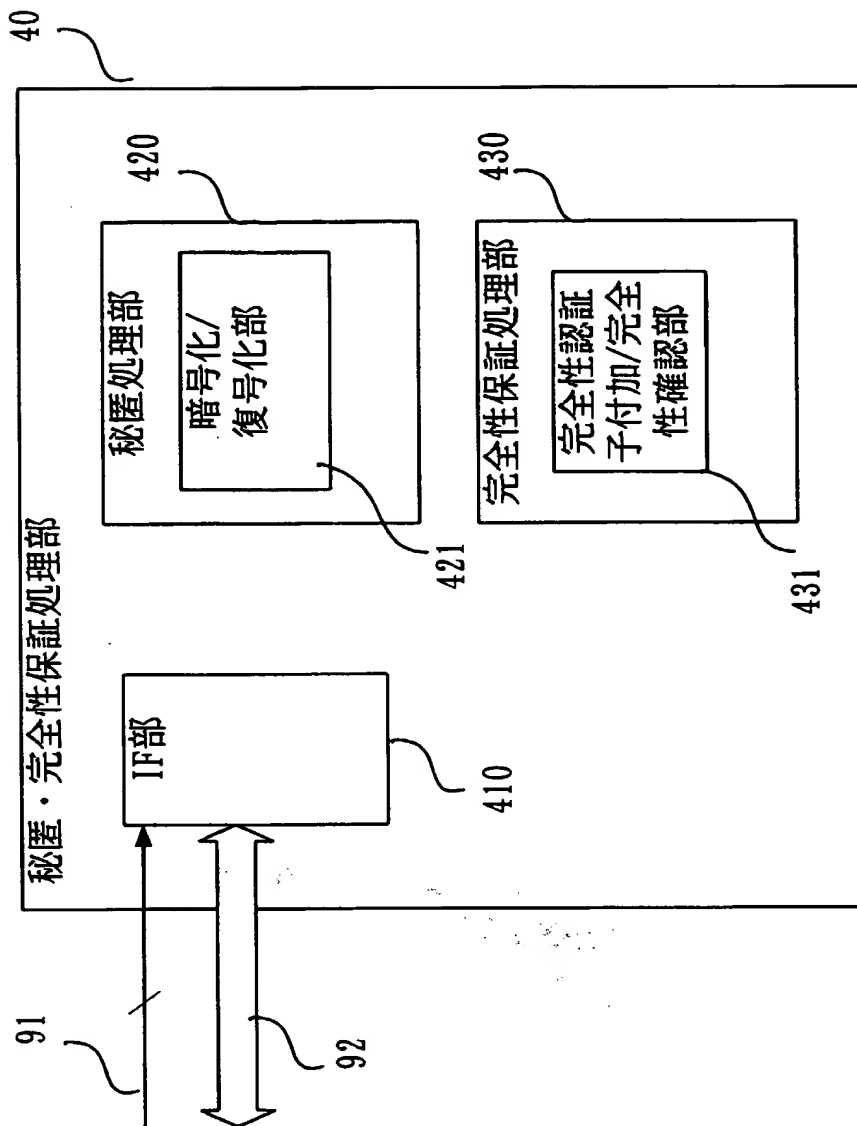
図 4



THIS PAGE BLANK (USPTO)

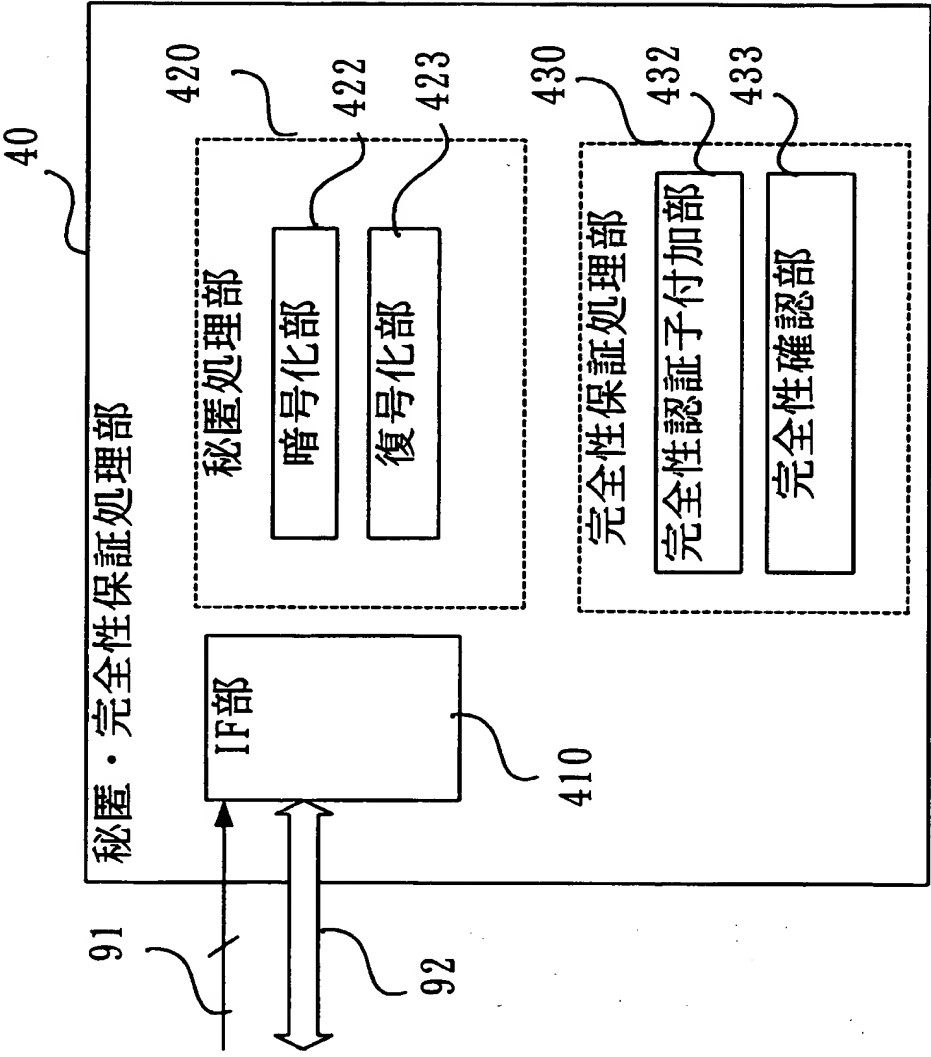
5 / 24

図 5



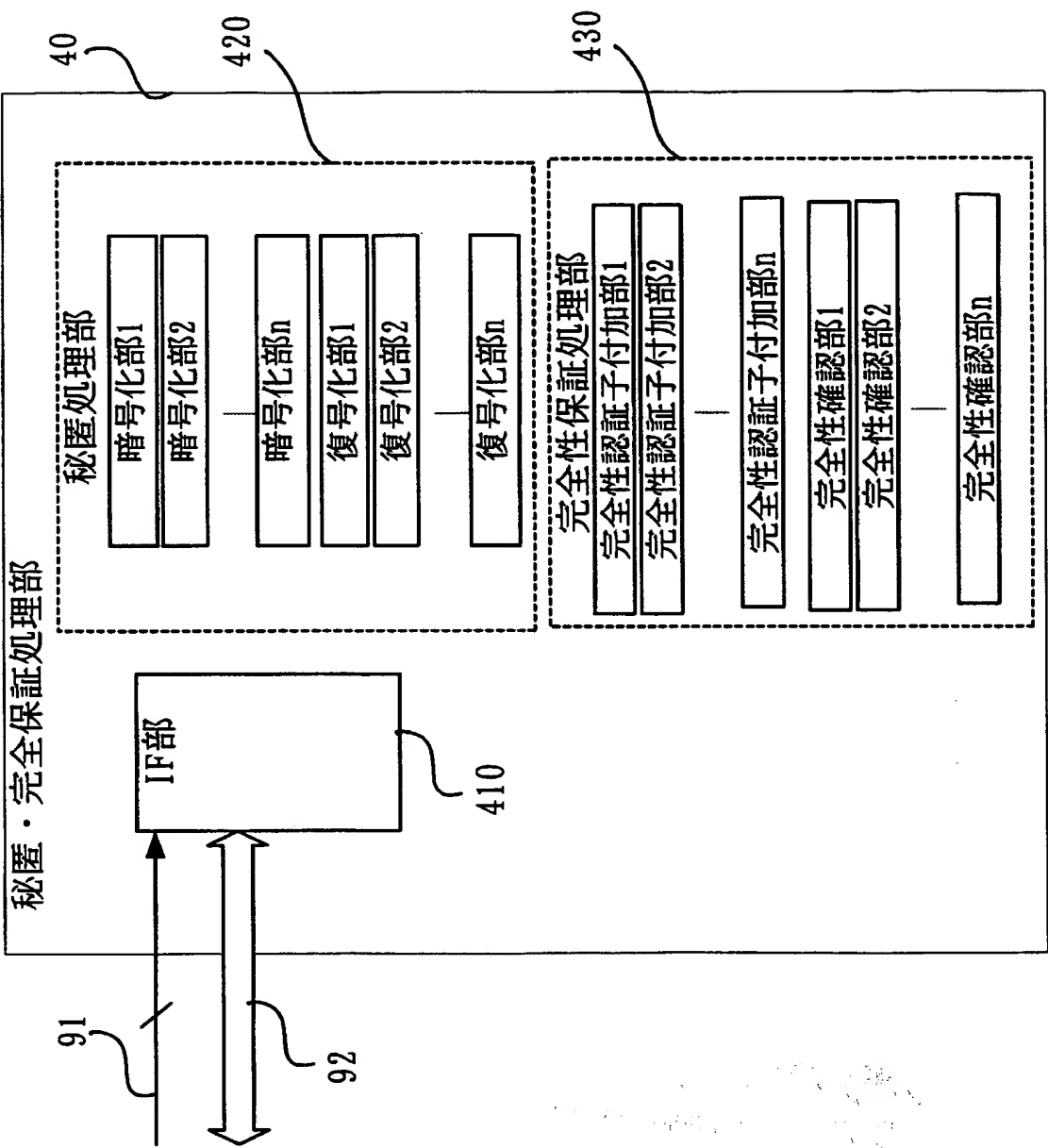
THIS PAGE BLANK (USPTO)

図 6



THIS PAGE BLANK (USPTO)

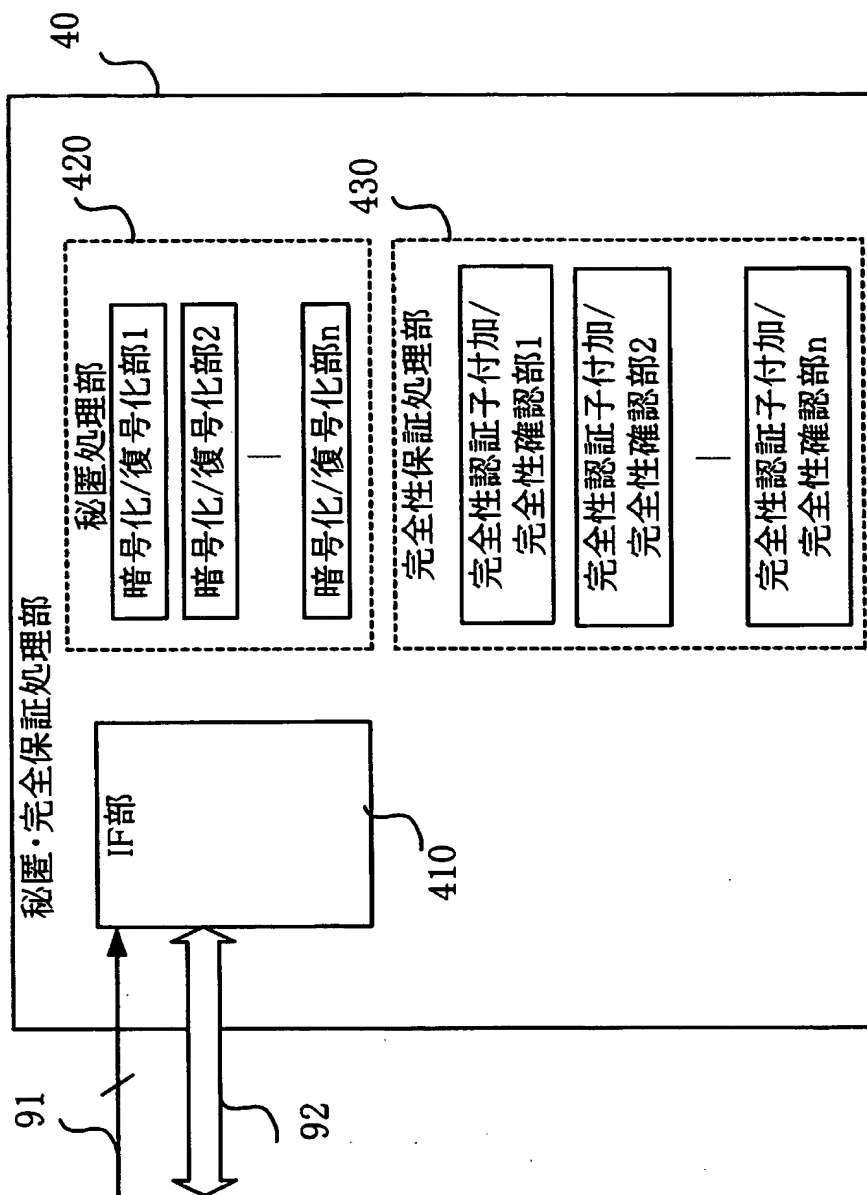
図 7



THIS PAGE BLANK (USPTO)

8 / 24

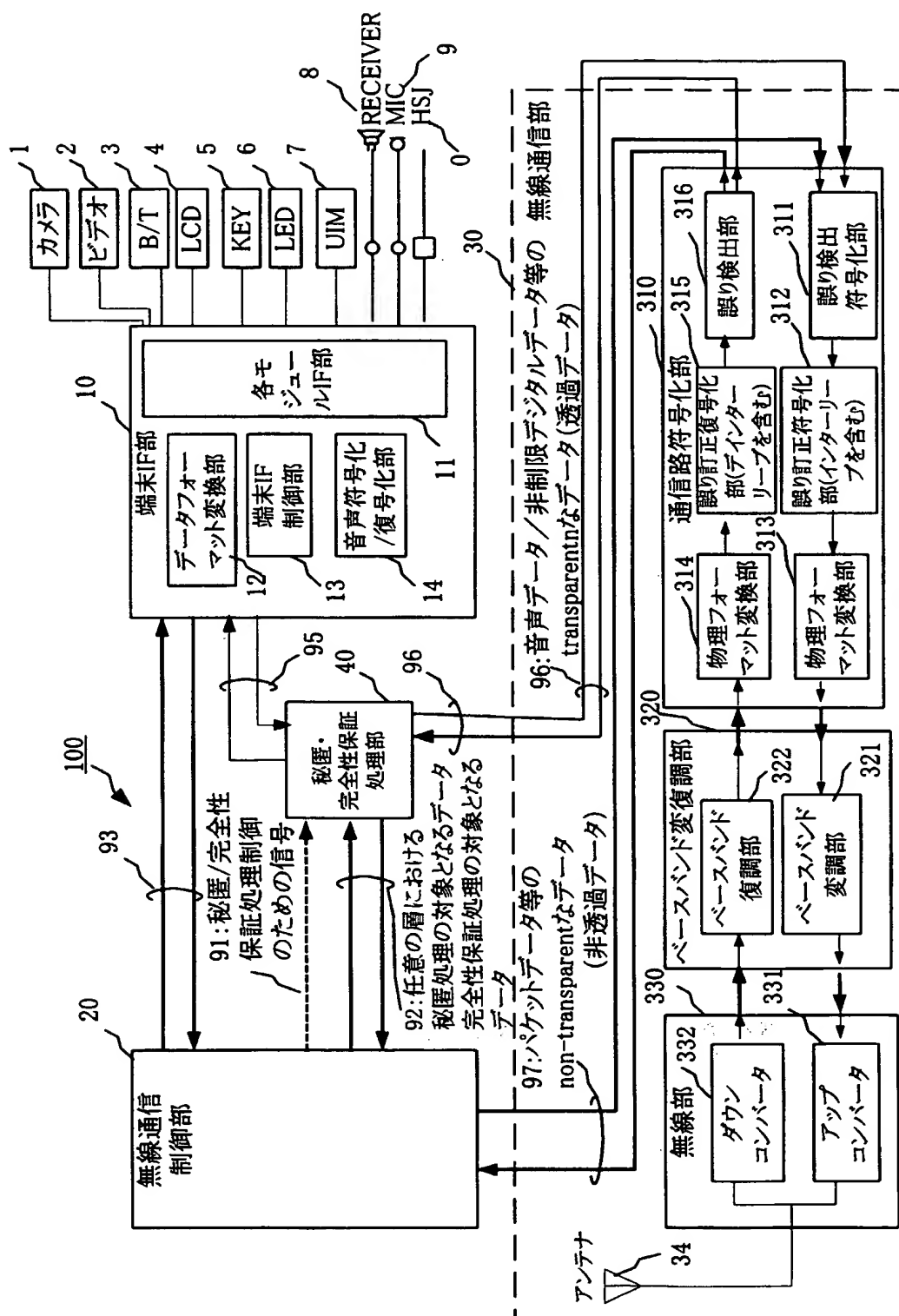
図 8



THIS PAGE BLANK (USPTO)

9/24

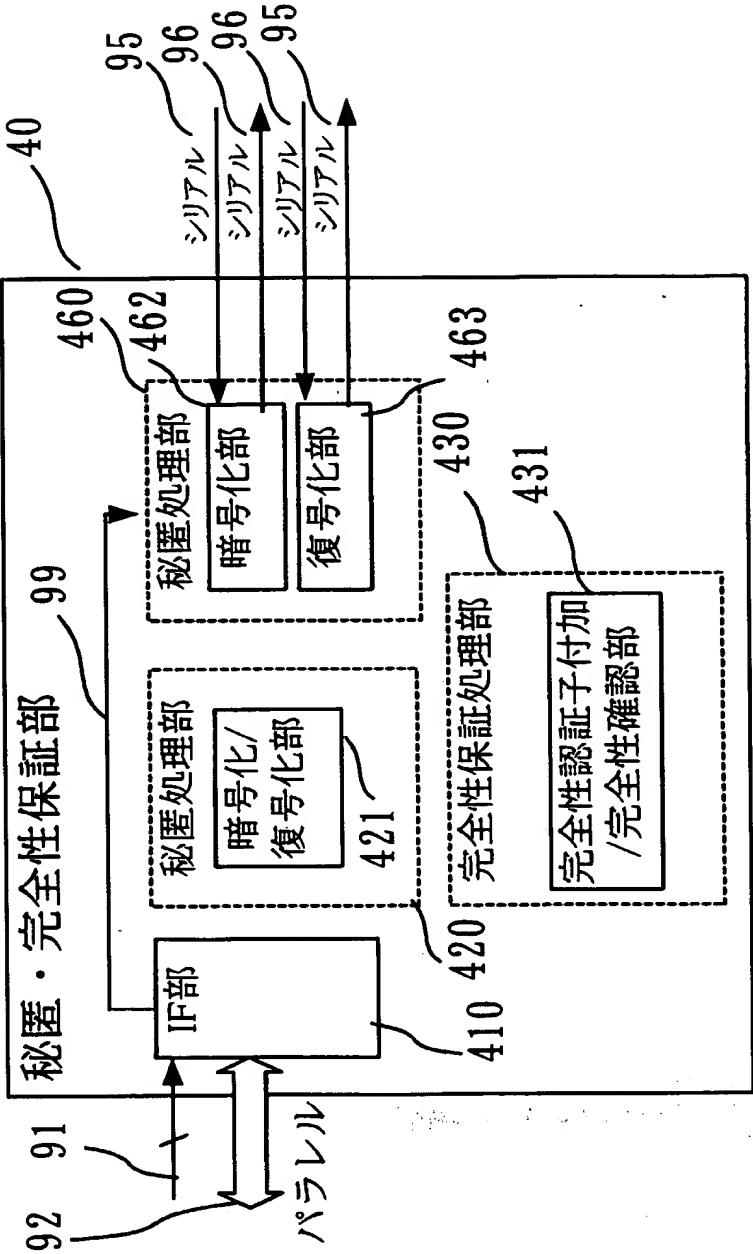
図 9



THIS PAGE BLANK (USPTO)

10 / 24

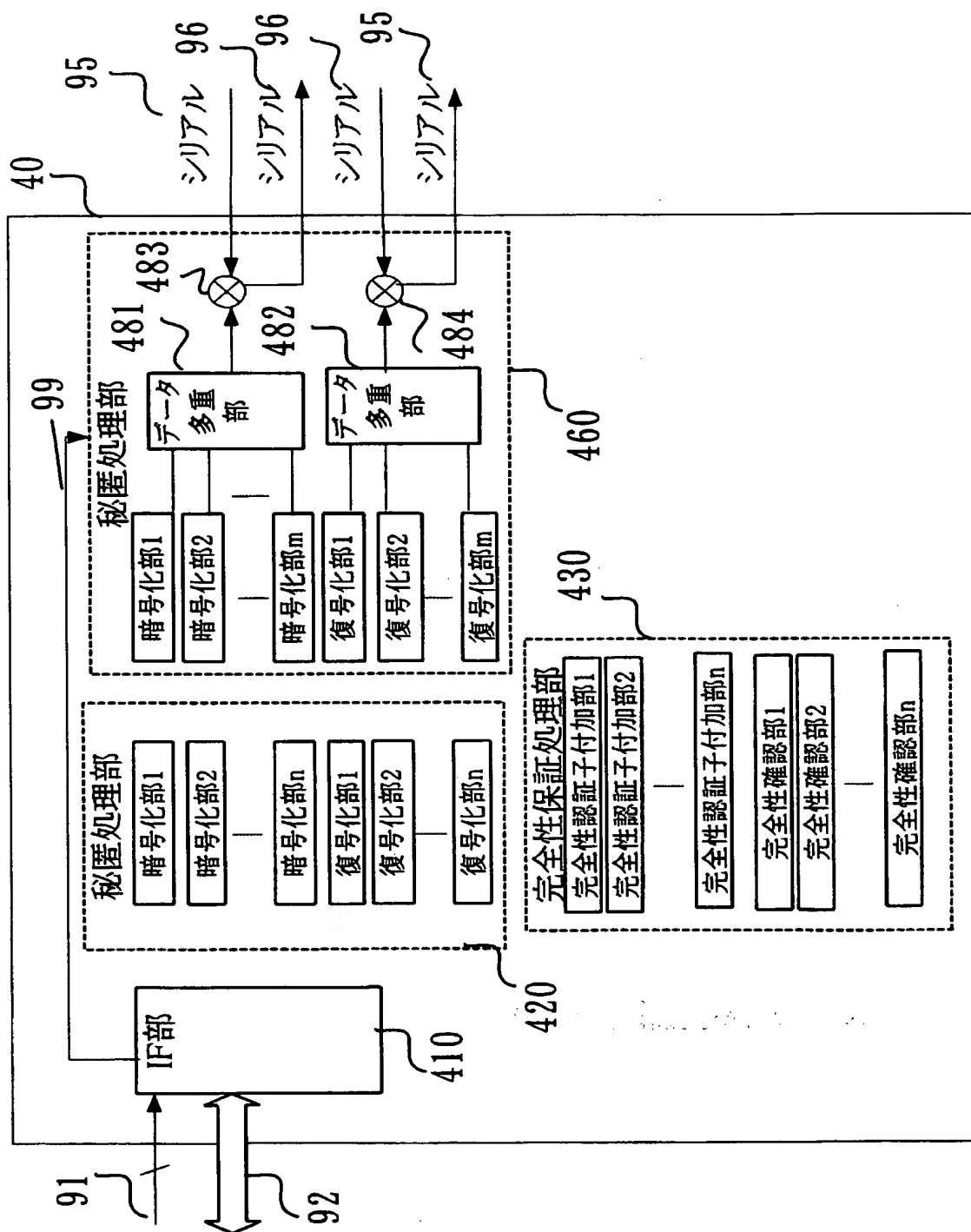
図 10



THIS PAGE BLANK (USPTO)

11 / 24

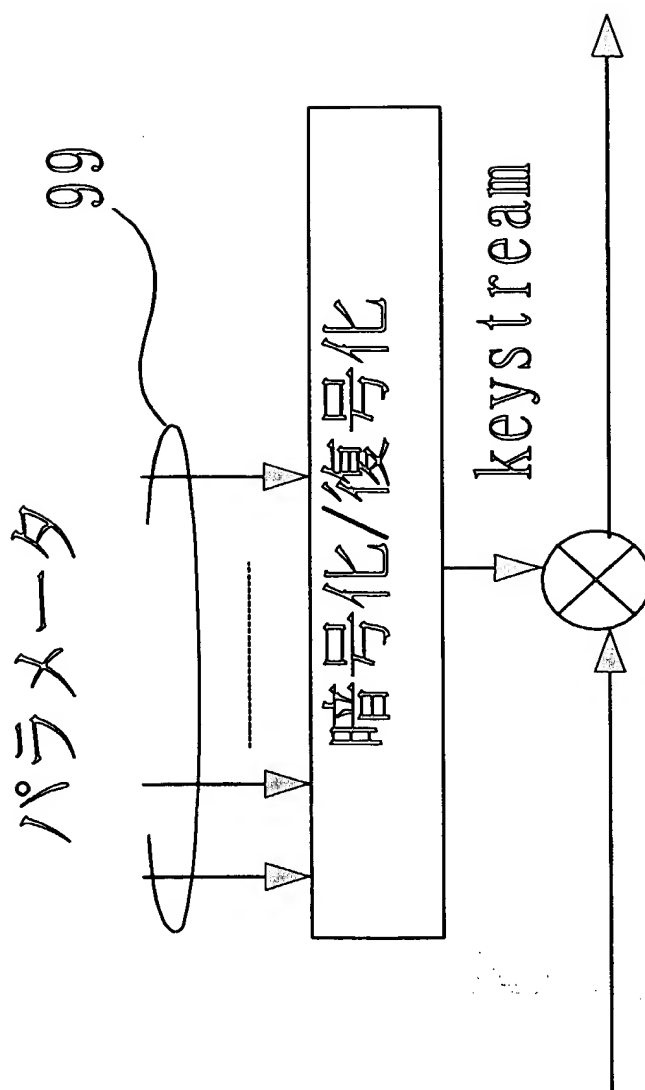
図 11



THIS PAGE BLANK (USPTO)

12 / 24

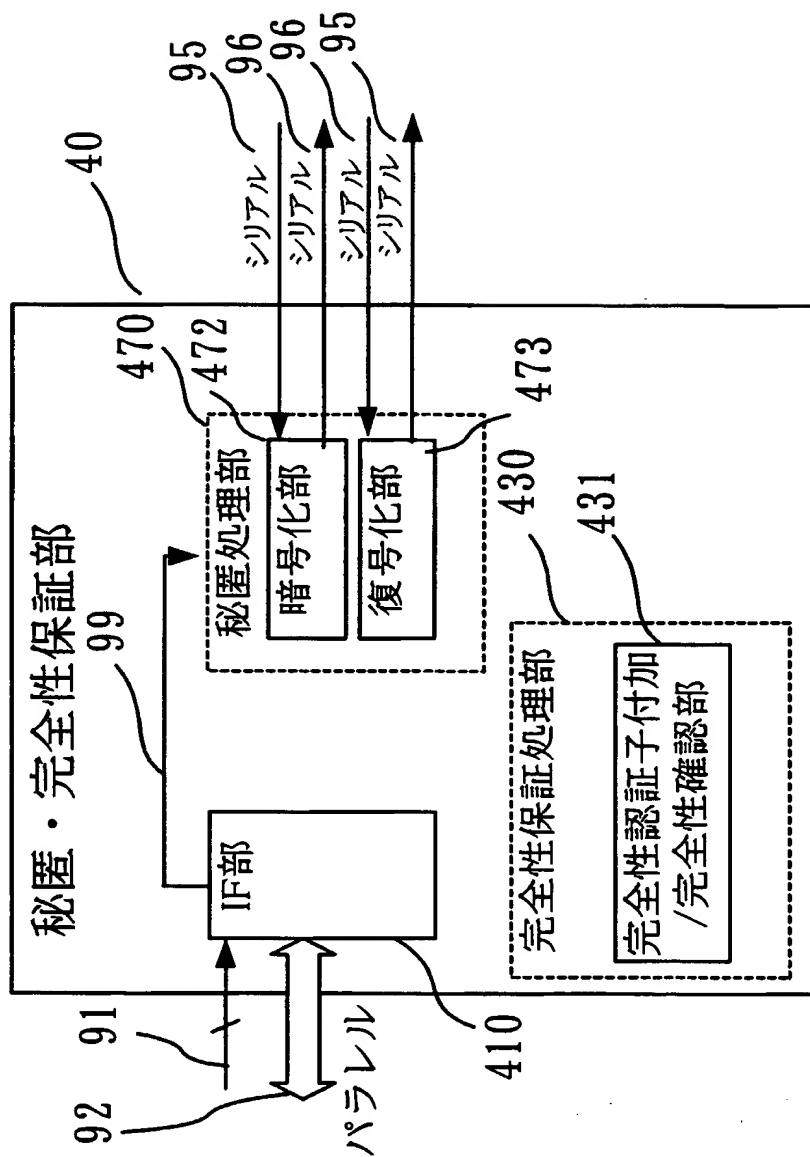
図 12



THIS PAGE BLANK (USPTO)

13 / 24

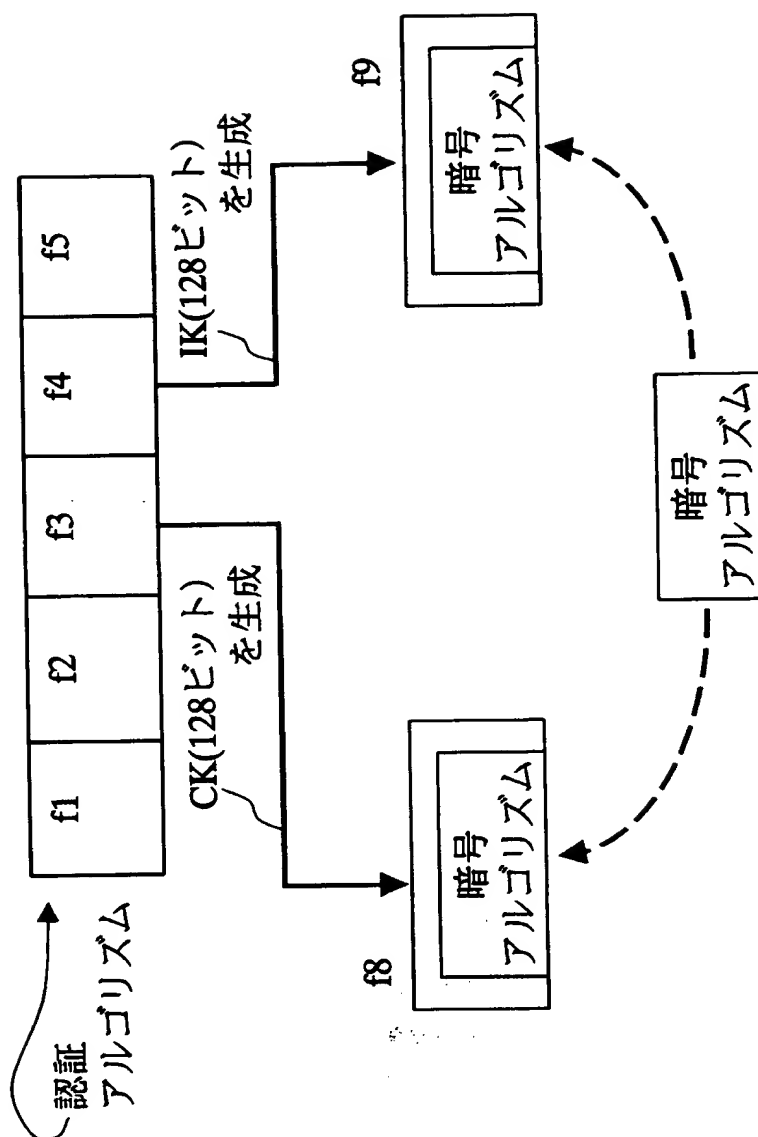
図 13



THIS PAGE BLANK (USPTO)

14 / 24

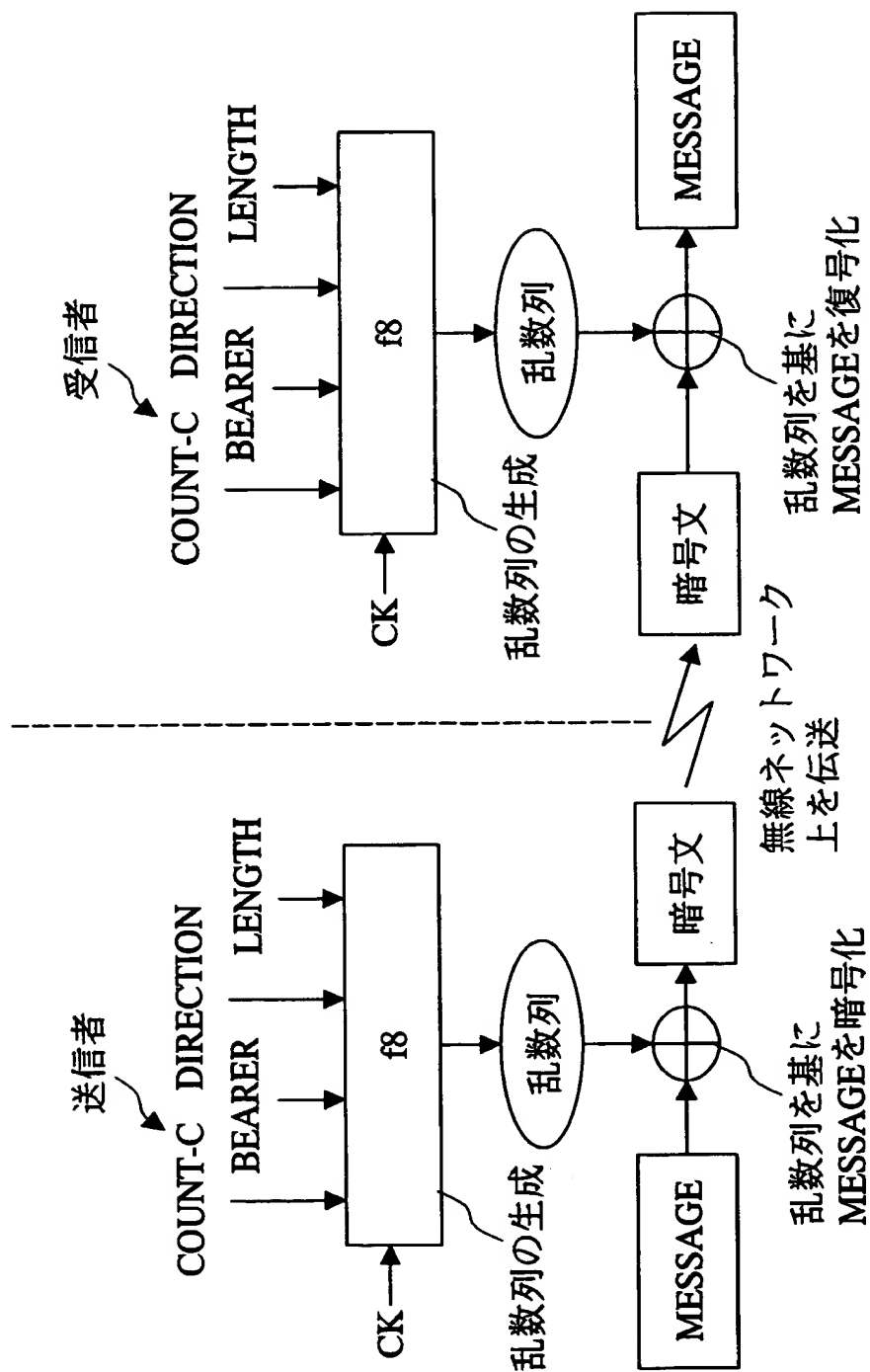
図 14



THIS PAGE BLANK (USPTO)

15 / 24

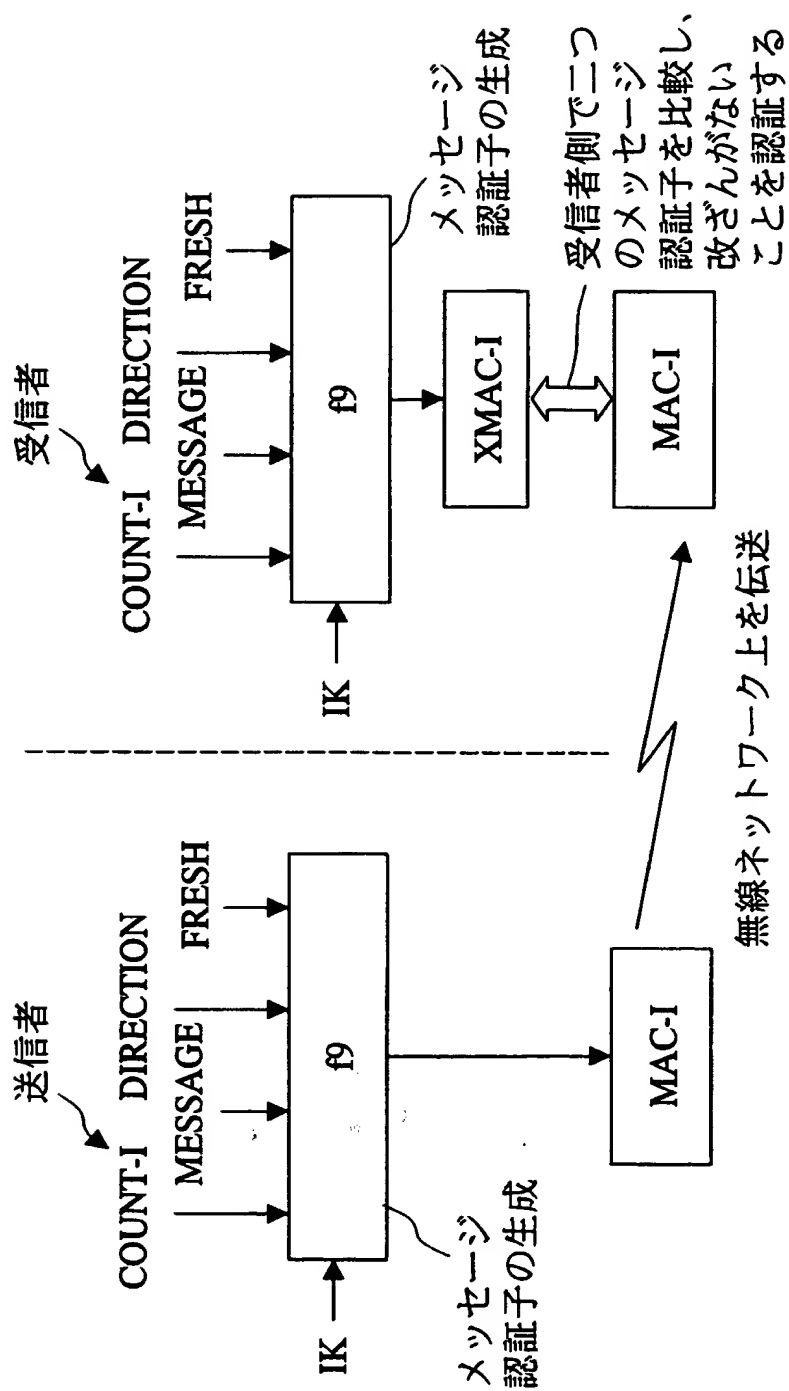
図 15



THIS PAGE BLANK (USPTO)

16 / 24

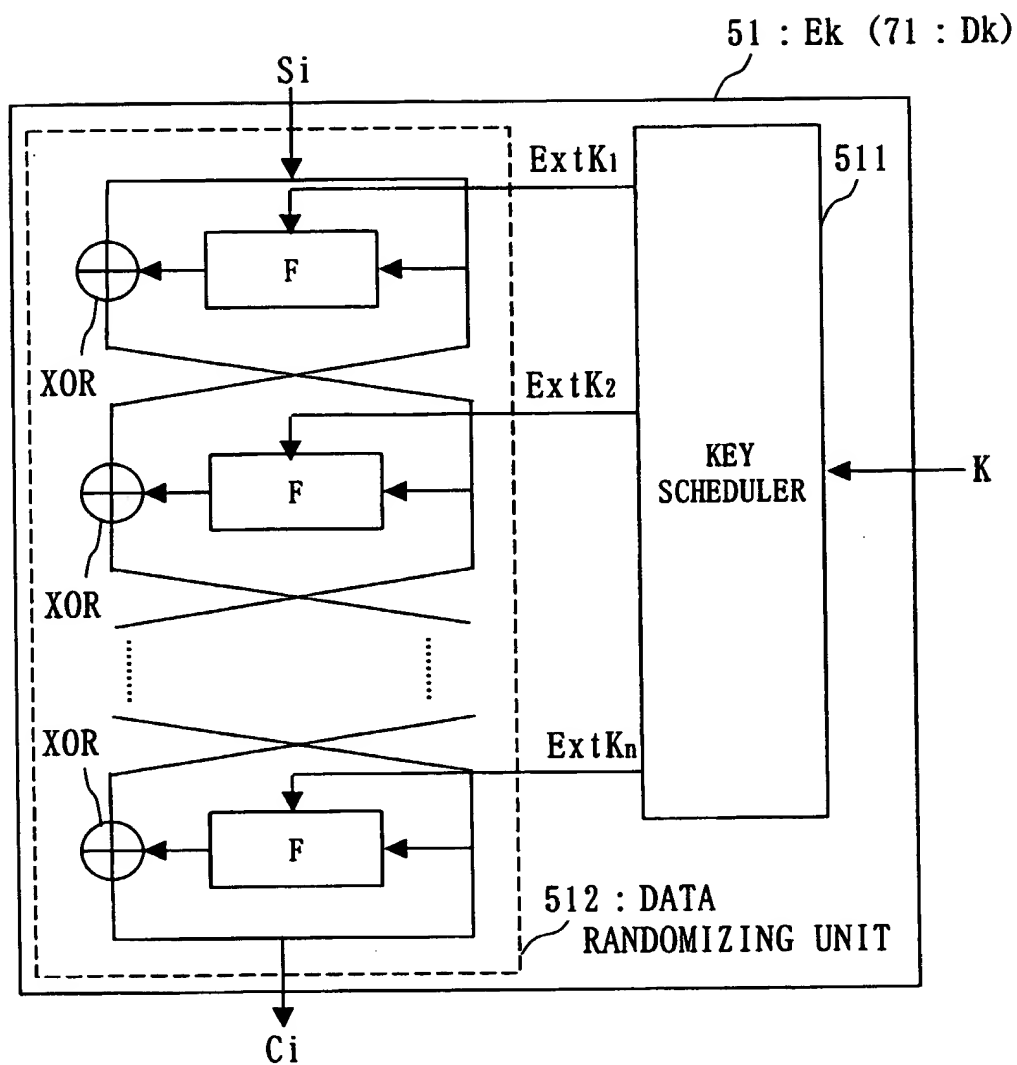
図 16



THIS PAGE BLANK (USPTO)

17/24

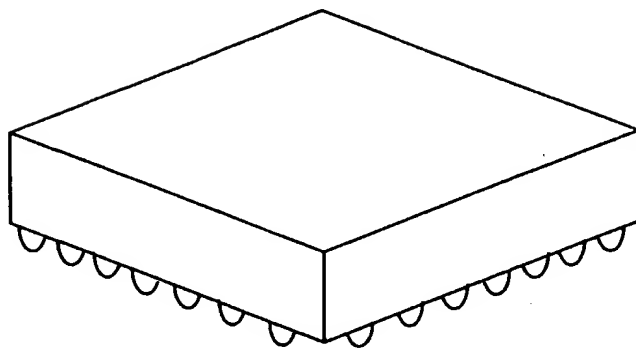
図17



THIS PAGE BLANK (USPTO)

18/24

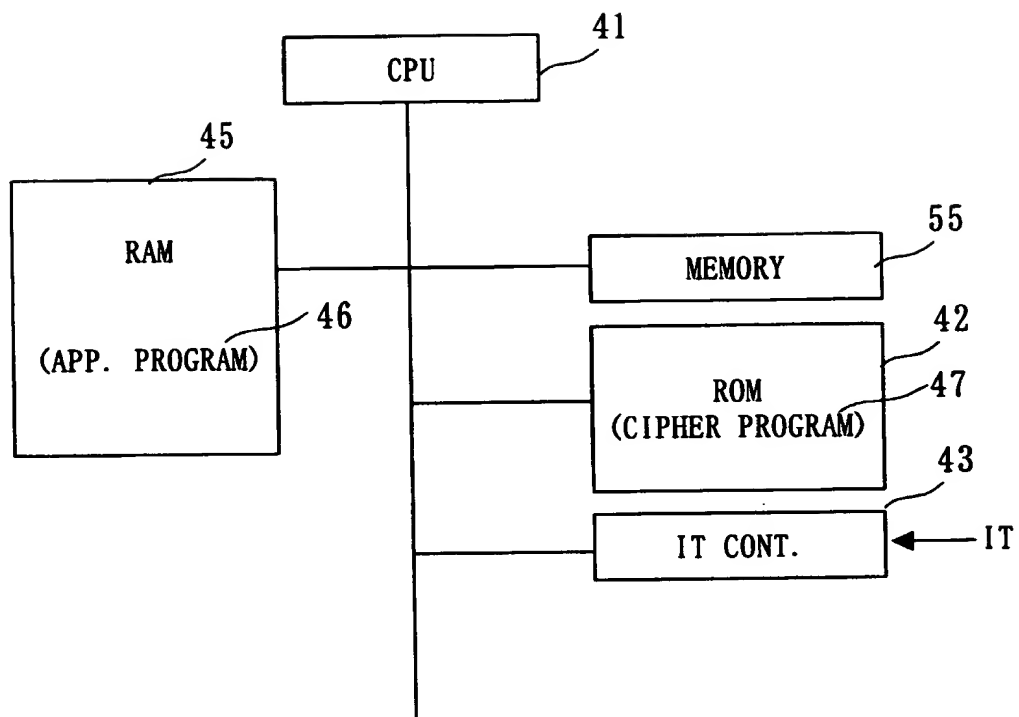
図18



THIS PAGE BLANK (USPTO)

19/24

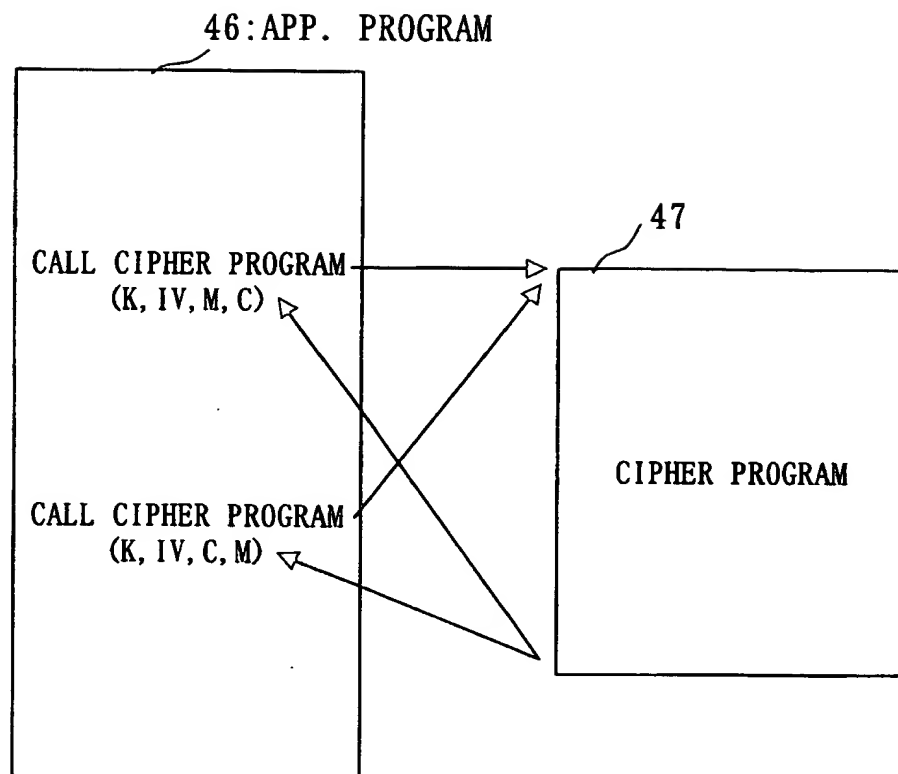
図 19



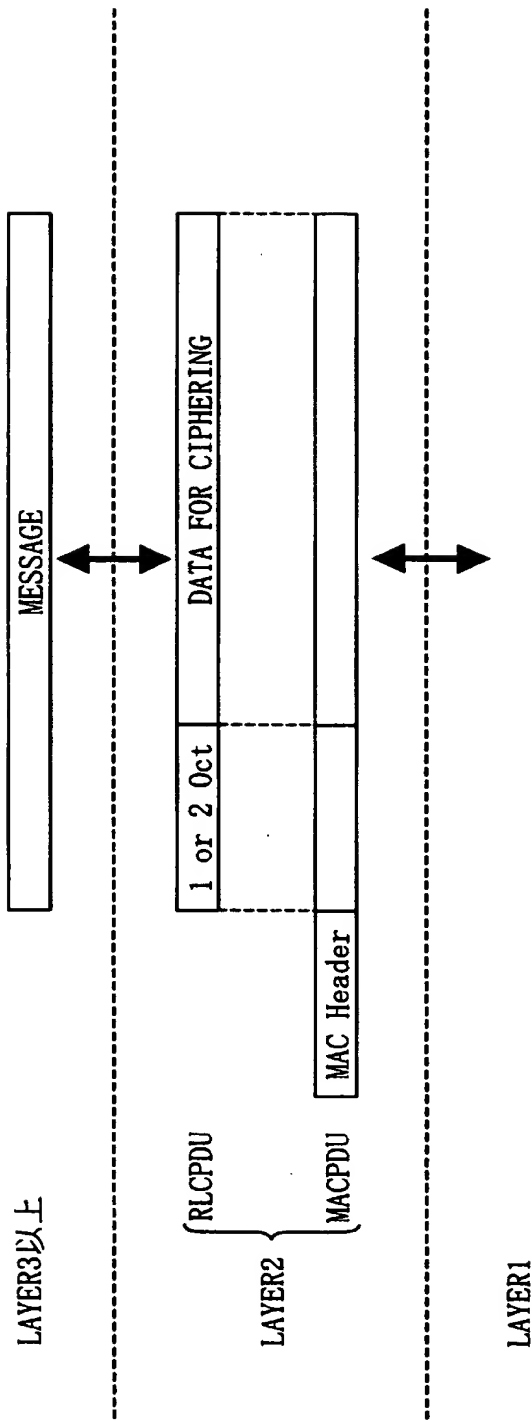
THIS PAGE BLANK (USPTO)

20/24

図 20



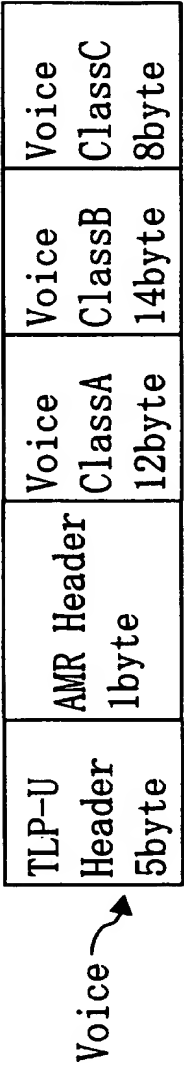
THIS PAGE BLANK (USPTO)



THIS PAGE BLANK (USPTO)

22/24

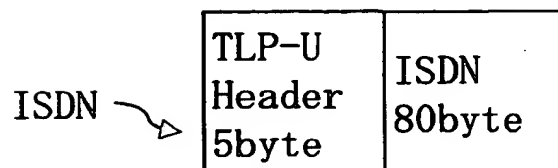
図22



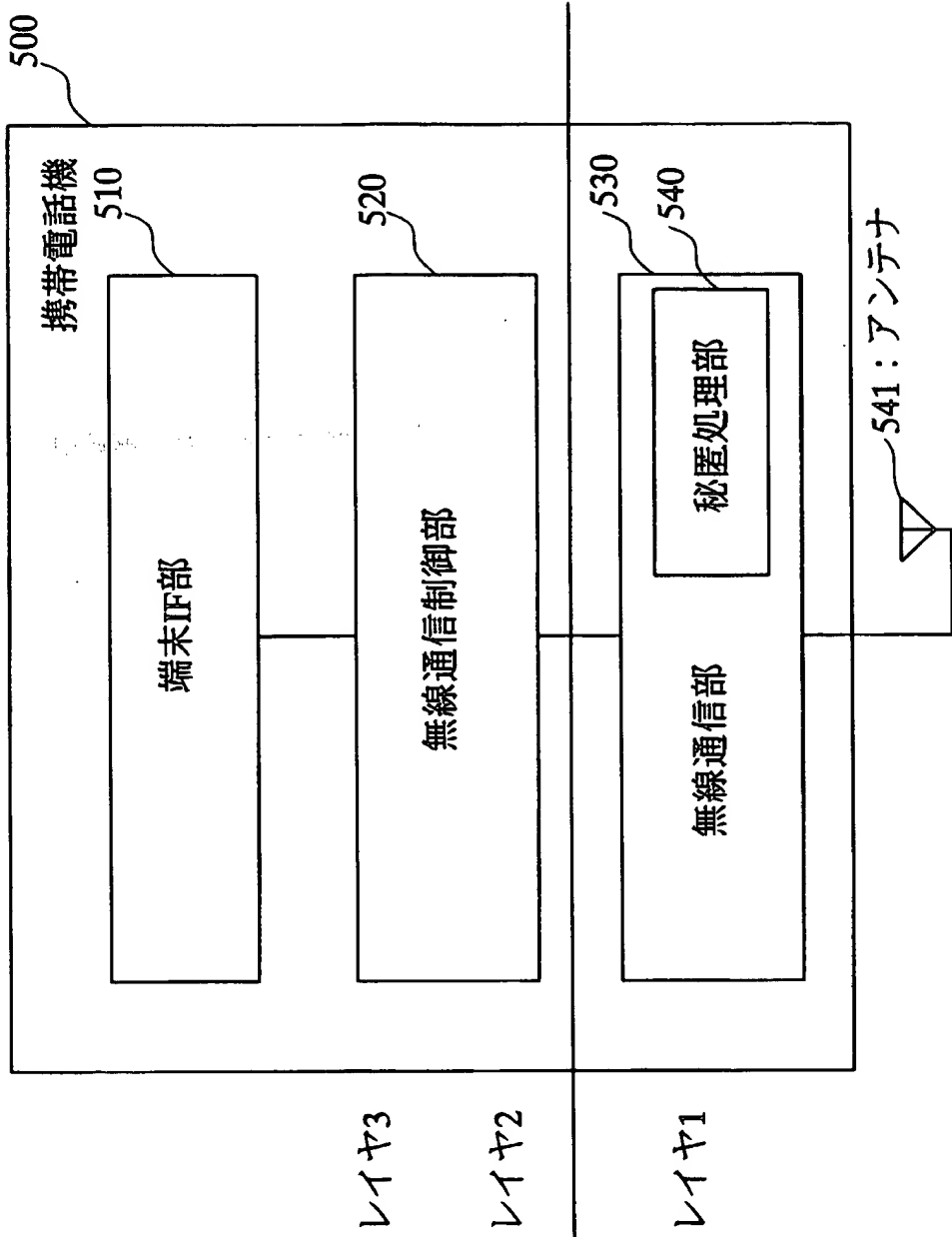
THIS PAGE BLANK (USPTO)

23/24

☒23



THIS PAGE BLANK (USPTO)



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09128

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04Q 7/38, H04L 9/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04B 7/24-7/26, H04Q 7/00, G09C 1/00-5/00,
H04K 1/00-3/00, H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-22996, A (Mitsubishi Electric Corporation), 23 January, 1998 (23.01.98) & GB, 2314741, A & CA, 2205637, A & DE, 19721949, A1 & US, 6016350, A	1-38
Y	JP, 7-245606, A (NEC Corporation), 19 September, 1995 (19.09.95) (Family: none)	1-38
Y	JP, 7-327257, A (Hitachi, Ltd.), 12 December, 1995 (12.12.95) (Family: none)	1-38
Y	JP, 10-66157, A (Nokia Mobile Phones Ltd.), 06 March, 1998 (06.03.98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111, A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	JP, 5-22284, A (Kokusai Electric Co., Ltd.), 29 January, 1993 (29.01.93) (Family: none)	1-38



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 12 March, 2001 (12.03.01)	Date of mailing of the international search report 21 March, 2001 (21.03.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	D. W. Davies and W. L. Price; Translation supervised by Tadahiro Uezono "Network Security", Nikkei McGraw Hill (1985), pp. 77-78, pp.121-123	9,18,24-26

国際調査報告

国際出願番号 PCT/JPO0/09128

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷

H04Q 7/38 H04L 9/16

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷H04B 7/24-7/26 H04Q 7/00 G09C 1/00-5/00
H04K 1/00-3/00 H04L 9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 10-22996, A (三菱電機株式会社) 23. 1月. 1998 (23. 01. 98) & GB, 2314741, A & CA, 2205637, A & DE, 19721949, A1 & US, 6016350, A	1-38
Y	JP, 7-245606, A (日本電気株式会社) 19. 9月. 1995 (19. 09. 95), (ファミリーなし)	1-38

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

12. 03. 01

国際調査報告の発送日

21.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政



5W

9570

電話番号 03-3581-1101 内線 3574

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 7-327257, A (株式会社日立製作所) 12. 12月. 1995 (12. 12. 95), (ファミリーなし)	1-38
Y	JP, 10-66157, A (ノキア モービル フォーンズ リミテッド) 6. 3月. 1998 (06. 03. 98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111, A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	JP, 5-22284, A (国際電気株式会社) 29. 1月. 1993 (29. 01. 93), (ファミリーなし)	1-38
Y	D. W. Davies and W. L. Price著, 上園忠弘監訳 「ネットワーク・セキュリティ」日経マグロウヒル, (昭和60年), pp. 77-78及び121-123	9, 18, 24-26